Draft updated Guidance for a risk-based approach to virtual assets and VASPs

Table of contents

Acronyms

AEC	Anonymity-Enhanced Cryptocurrency
AML	Anti-Money Laundering
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
CPF	Counter-proliferation financing
DApp	Decentralised or distributed application
DNFBP	Designated Non-Financial Business and Profession
ICO	Initial Coin Offering
FI	Financial institution
FIU	Financial intelligence unit
ML	Money Laundering
MSB	Money Services Business
MVTS	Money or Value Transfer Service
OTC	Over-the-Counter
P2P	Peer-to-Peer
PEP	Politically exposed person
PF	Proliferation financing
~~**RBA**~~	~~Risk-Based Approach~~
SRB	Self-regulatory body
STR	Suspicious transaction report
TF	Terrorist Financing
VA	Virtual Asset
VASP	Virtual Asset Service Provider

Executive summary

In October 2018, the Financial Action Task Force (FATF) adopted changes to its Recommendations to explicitly clarify that they apply to financial activities involving virtual assets, and also added two new definitions in the Glossary, "virtual asset" (VA) and "virtual asset service provider" (VASP). The amended FATF Recommendation 15 requires that VASPs be regulated for anti-money laundering and combating the financing of terrorism (AML/CFT) purposes, licenseced or registered, and subject to effective systems for monitoring or supervision.

In June 2019, the FATF adopted an Interpretive Note to Recommendation 15 to further clarify how the FATF requirements should apply in relation to VAs and VASPs, in particular with regard to the application of the risk-based approach (RBA) to VA activities or operations and VASPs; supervision or monitoring of VASPs for AML/CFT purposes; licensing or registration; preventive measures, such as customer due diligence, recordkeeping, and suspicious transaction reporting, among others; sanctions and other enforcement measures; and international co-operation.

The FATF also adopted an earlier version of this the present Guidance[1] on the application of the RBA risk-based approach to VAs and VASPs iIn June 2019. It is intended to both help both national authorities in understanding and developing regulatory and supervisory responses to VA activities and VASPs, and to help private sector entities seeking to engage in VA activities, in understanding their AML/CFT obligations and how they can effectively comply with these requirements.

This Guidance outlines the need for countries and VASPs, and other entities involved in VA activities, to understand the money laundering and terrorist financing (ML/TF) risks associated with their VA activities and take appropriate mitigating measures to address themthose risks. In particular, the Guidance provides examples of risk indicators that should specifically be considered in a VA context, with an emphasis on factors that would further obfuscate transactions or inhibit VASPs' ability to identify customers.

The Guidance examines how VA activities and VASPs fall within the scope of the FATF Recommendations. It discusses the five types of activities covered by the VASP definition and provides examples of VA-related activities that would fall within the VASP definition and also those that would potentially be excluded from the FATF scope. In that respect, it highlights the key elements required to qualify as a VASP, namely acting as a business on behalf of the customers and actively facilitating VA-related activities.

The Guidance describes the application of the FATF Recommendations to countries and competent authorities; as well as to VASPs and other obliged entities that engage into VA activities, including financial institutions such as banks and securities broker-dealers, among others. Almost all of the FATF Recommendations are directly relevant to address the ML/TF risks associated with VAs and VASPs, while other Recommendations are less directly or explicitly linked to VAs or VASPs, though they are still relevant and applicable. VASPs therefore have the same full set of obligations as financial institutions andor DNFBPsdesignated non-financial businesses and professions.

The Guidance details the full range of obligations applicable to VASPs as well as to VAs under the FATF Recommendations, following a Recommendation-by-Recommendation approach. This includes clarifying that all of the funds or value-based terms in the FATF Recommendations (*e.g.*, "property," "proceeds," "funds," "funds or other assets," and other

[1] This Guidance updates the 2015 *FATF Guidance for a Risk-Based Approach to Virtual Currencies*.

"corresponding value") include VAs. Consequently, countries should apply all of the relevant measures under the FATF Recommendations to VAs, VA activities, and VASPs.

The Guidance explains the VASP registration or licensing requirements, in particular how to determine in which country/ies VASPs should be registered or licensed – at a minimum where they were created; or in the jurisdiction where their business is located in cases where they are a natural person, but jurisdictions can also choose to require VASPs to be licensed or registered before conducting business in their jurisdiction or from their jurisdiction. The Guidance further underlines that national authorities are required to take action to identify natural or legal persons that carry out VA activities without the requisite license or registration. This would be equally applicable ~~by~~ to countries ~~which~~ that have chosen to prohibit VA and VA activities at the national level.

Regarding VASP supervision, the Guidance makes clear that only competent authorities, and not self-regulatory bodies, can act as VASP supervisory or monitoring bodies~~;, and not self-regulatory bodies.~~ They should conduct risk-based supervision or monitoring, with adequate powers, including the power to conduct inspections, compel the production of information and impose sanctions. There is a specific focus on the importance of international co-operation between supervisors, given the cross-border nature of VASPs' activities and provision of services.

The Guidance makes clear that VASPs, and other entities involved in VA activities, need to apply all the preventive measures described in FATF Recommendations 10 to 21. The Guidance explains how these obligations should be fulfilled in a VA context and provides clarifications regarding the specific requirements applicable ~~regarding~~ to the USD/EUR 1 000 threshold for VA occasional transactions, above which VASPs must conduct customer due diligence (Recommendation 10); and the obligation to obtain, hold, and transmit required originator and beneficiary information, immediately and securely, when conducting VA transfers (Recommendation 16) (the 'travel rule'). As the guidance makes clear, relevant authorities should co-ordinate to ensure this can be done in a way that is compatible with national data protection and privacy rules.

Finally, the Guidance provides examples of jurisdictional approaches to regulating, supervising, and enforcing VA activities, VASPs, and other obliged entities for AML/CFT.

In [*June 2021*], this Guidance was updated to provide the public and private sectors with revised guidance. These revisions focused on six key areas where greater guidance from the FATF was sought. These are to (1) clarify the definitions of VA and VASP to make clear that these definitions are expansive and there should not be a case where a relevant financial asset is not covered by the FATF Standards (either as a VA or as a traditional financial asset), (2) provide guidance on how the FATF Standards apply to so-called stablecoins, (3) provide additional guidance on the risks and potential risk mitigants for peer-to-peer transactions, (4) provide updated guidance on the licensing and registration of VASPs, (5) provide additional guidance for the public and private sectors on the implementation of the 'travel rule', and (6) include Principles of Information-Sharing and Co-operation Amongst VASP Supervisors. This document incorporates and supersedes the 2019 Guidance.

Section I - Introduction

Background

1. New technologies, products, and related services have the potential to spur financial innovation and efficiency and improve financial inclusion, but they also create new opportunities for criminals and terrorists to launder their proceeds or finance their illicit activities. The risk-based approach is central to the effective implementation of the revised Financial Action Task Force (FATF) International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, which FATF members adopted in 2012, and the FATF therefore actively monitors the risks relating to new technologies. The monitoring of new and emerging risks, including the risks relating to new technologies, should inform the risk assessment process of countries and obliged entities and, as per the risk-based approach, should guide the allocation of resources as appropriate to mitigate these risks.
2. In June 2014, the FATF issued *Virtual Currencies: Key Definitions and Potential AML/CFT Risks* in response to the emergence of virtual currencies and their associated payment mechanisms for providing new methods of transmitting value over the Internet. In June 2015, the FATF issued the *Guidance for a Risk-Based Approach to Virtual Currencies* (the 2015 VC Guidance) as part of a staged approach to addressing the money laundering and terrorist financing (ML/TF) risks associated with virtual currency payment products and services.
3. The 2015 VC Guidance focuses on the points where virtual currency activities intersect with and provide gateways to and from (*i.e.,* the on and off ramps to) the traditional regulated financial system, in particular convertible virtual currency exchangers. In recent years, however, the virtual asset space has evolved to include a range of new products and services, business models, and activities and interactions, including virtual-to-virtual asset transactions.
4. In particular, the virtual asset ecosystem has seen the rise of anonymity-enhanced cryptocurrencies (AECs), mixers and tumblers, decentralized platforms and exchanges, and other types of products and services that enable or allow for reduced transparency and increased obfuscation of financial flows, as well as the emergence of other virtual asset business models or activities such as initial coin offerings (ICOs) that present ML/TF ~~risks~~, ~~including~~ fraud and market manipulation risks. Further, new illicit financing typologies continue to emerge, including the increasing use of virtual-to-virtual layering schemes that attempt to further obfuscate transactions in a comparatively easy, cheap, and secure manner.
5. Given the development of additional products and services and the introduction of new types of providers in this space, the FATF recognized the need for further clarification on the application of the FATF Standards to new technologies and providers. In particular, in October 2018, the FATF adopted two new Glossary definitions—"virtual asset" (VA) and "virtual asset service provider" (VASP)—and updated Recommendation 15 (see Annex A). The objectives of those changes were to further clarify the application of the FATF Standards to VA activities and VASPs in order to ensure a level regulatory playing field for VASPs globally and to assist jurisdictions in mitigating the ML/TF risks associated with VA activities and in protecting the integrity of the global financial system. The FATF also clarified that the Standards apply to both virtual-to-virtual and virtual-to-fiat transactions and interactions involving VAs.

6. In June 2019, the FATF adopted an Interpretive Note to Recommendation 15 (INR. 15) to further clarify how the FATF requirements should apply in relation to VAs and VASPs, in particular with regard to the application of the risk-based approach to VA activities or operations and VASPs; supervision or monitoring of VASPs for anti-money laundering and countering the financing of terrorism (AML/CFT) purposes; licensing or registration; preventive measures, such as customer due diligence, recordkeeping, and suspicious transaction reporting, among others; sanctions and other enforcement measures; and international co-operation (see Annex A).

7. The FATF adopted this Guidance at its June 2019 Plenary. Following the adoption of this Guidance and the revisions to the FATF Standards, the FATF continued its enhanced monitoring of the VA sector and the implementation of the revised Standards by countries. In June 2020, the FATF completed its *12-Month Review of the Revised FATF Standards on VAs and VASPs* and released its findings in a report. This report found that, overall, both the public and private sectors had made progress in implementing the revised FATF Standards. The report found, however, challenges remain, with some jurisdictions' AML/CFT regimes for VASPs not yet established or not yet operational. The report also identified areas where greater FATF guidance was necessary to clarify the application of the revised FATF Standards. Simultaneously with this report, the FATF also released its *Report to the G20 on So-called Stablecoins*. This report sets out how the revised FATF Standards apply to so-called stablecoins and considers the AML/CFT issues. In September 2020, the FATF also released a report on *VA Red Flag Indicators of ML/TF* for use by the public and private sectors. Finally, in March 2021, the FATF released its *Guidance on a Risk-Based Approach to AML/CFT Supervision*. While this report addresses AML/CFT supervision broadly, it includes a compendium of information for the AML/CFT supervision of VASPs specifically.

~~7.~~8. The 12-month review report and G20 report both committed the FATF to release updated Guidance for the public and private sector on the revised FATF Standards and their application to VAs and VASPs. In particular, these two reports set out six main areas where greater Guidance was sought. To address these six areas, this Guidance was updated in [*June 2021]* to (1) clarify the definitions of VA and VASP to make clear that these definitions are expansive and there should not be a case where a relevant financial asset is not covered by the FATF Standards (either as a VA or as a traditional financial asset), (2) provide guidance on how the FATF Standards apply to so-called stablecoins, (3) provide additional guidance on the risks and potential risk mitigants for peer-to-peer transactions, (4) provide updated guidance on the licensing and registration of VASPs, (5) to provide additional guidance for the public and private sectors on the implementation of the 'travel rule' and (6) to include Principles of Information-Sharing and Co-operation Amongst VASP Supervisors. The Guidance was also updated to reflect the passage of time and the publication of the other FATF reports, including those outlined above. The updates to this Guidance are summarised in Annex B.

Purpose of the Guidance

~~8.~~9. This updated Guidance expands on the 2015 VC Guidance and further explains the application of the risk-based approach to AML/CFT measures for VAs; identifies the entities that conduct activities or operations relating to VA—*i.e.*, VASPs; and clarifies the application of the FATF Recommendations to VAs and VASPs. The Guidance is intended to help national authorities in understanding and developing regulatory responses to covered VA activities and VASPs, including by amending national laws, where applicable,

in their respective jurisdictions in order to address the ML/TF risks associated with covered VA activities and VASPs.

~~9.~~10. The Guidance also is intended to help private sector entities seeking to engage in VA activities or operations as defined in the FATF Glossary to better understand their AML/CFT obligations and how they can effectively comply with the FATF requirements. It provides guidelines to countries, competent authorities, and industry for the design and implementation of a risk-based AML/CFT regulatory and supervisory framework for VA activities and VASPs, including the application of preventive measures such as customer due diligence, record-keeping, and suspicious transaction reporting, among other measures.

~~10.~~11. The Guidance incorporates the terms adopted by the FATF in October 2018 and readers are referred to the FATF Glossary definitions for "virtual asset" and "virtual asset service provider" (Annex A).

~~11.~~12. The Guidance seeks to explain how the FATF Recommendations should apply to VA activities and VASPs; provides examples, where relevant or potentially most useful; and identifies obstacles to applying mitigating measures alongside potential solutions. It is intended to serve as a complement to Recommendation 15 on New Technologies (R. 15) and its Interpretive Note, which describe the full range of obligations applicable to VASPs as well as to VAs under the FATF Recommendations, including the Recommendations relating to "property," "proceeds," "funds," "funds or other assets," and other "corresponding value." In doing so, the Guidance supports the effective implementation of national AML/CFT measures for the regulation and supervision of VASPs (as well as other obliged entities) and the covered VA activities in which they engage and the development of a common understanding of what a risk-based approach to AML/CFT entails.

~~12.~~13. While the FATF notes that ~~some governments~~ some countries have implemented~~are considering a range of regulatory responses to VAs and to the regulation of~~ regulatory regimes for VAs and VASPs, ~~many~~ many jurisdictions ~~do not yet have in place~~have not yet put in place effective AML/CFT frameworks for mitigating the ML/TF risks associated with VA activities in particular, even as VA activities develop globally and VASPs increasingly operate across jurisdictions. The rapid development, increasing functionality, growing adoption, and global, cross-border nature of VAs therefore makes the urgent action by countries to mitigate the ML/TF risks presented by VA activities and VASPs a key priority of the FATF. While this Guidance is intended to facilitate the implementation of the risk-based approach to covered VA activities and VASPs for AML/CFT purposes, the FATF recognizes that other types of policy considerations, separate from AML/CFT, may come into play and shape the regulatory response to the VASP sector in individual jurisdictions.

Scope of the Guidance

~~13.~~14. The FATF Recommendations require all jurisdictions to impose specified, activities-based AML/CFT requirements on financial institutions (FIs), ~~and~~ designated non-financial businesses and professions (DNFBPs) and VASPs and ensure their compliance with those obligations. The FATF has agreed that all of the funds- or value-based terms in the FATF Recommendations (*e.g.*, "property," "proceeds," "funds," "funds or other assets," and other "corresponding value") include VAs and that countries should apply all of the relevant measures under the FATF Recommendations to VAs, VA activities, and VASPs. The primary focus of the Guidance is to describe how the Recommendations apply to VAs, VA activities, and VASPs in order to help countries better understand how they should implement the FATF Standards effectively.

15. Further, the Guidance focuses on VAs that are convertible ~~for~~ to other funds or value, including both VAs that are convertible to another VA and VAs that are convertible to fiat or that intersect with the fiat financial system~~, having regard to the VA and VASP definitions~~. It does not address other regulatory matters that are potentially relevant to VAs and VASPs (*e.g.*, consumer and investor protection, prudential safety and soundness, tax, anti-fraud or anti-market manipulation issues, network IT security standards, or financial stability concerns).

16. This Guidance also does not address central bank-issued digital currencies. For FATF's purposes, these are not VAs. The FATF Standards however apply to central bank digital currencies similar to any other form of fiat currency issued by a central bank.[2] Central bank digital currencies may have unique ML/TF risks compared with physical fiat currency, depending on their design. However, their non-inclusion in this Guidance does not indicate the FATF considers them unimportant. Rather, it is a product of the fact that they are categorized as fiat currency, rather than the VAs that this Guidance addresses.

~~1.~~

~~14.~~17. The Guidance recognizes that an effective risk-based approach will reflect the nature, diversity, and maturity of a country's VASP sector, the risk profile of the sector, the risk profile of individual VASPs operating in the sector and the legal and regulatory approach in the country, taking into account the cross-border, Internet-based nature and global reach of most VA activities. The Guidance sets out different elements that countries and VASPs should consider when designing and implementing a risk-based approach. When considering the general principles outlined in the Guidance, national authorities will have to take into consideration their national context, including the supervisory approach and legal framework as well as the risks present in their jurisdiction, again in light of the potentially global reach of VA activities.

~~15.~~18. The Guidance takes into account that just as illicit actors can abuse any institution that engages in financial activities, illicit actors can abuse VASPs engaging in VA activities, for ML, TF, sanctions evasion, fraud, and other nefarious purposes. The 2015 VC Guidance, the 2018 FATF Risk, Trends, and Methods Group papers relating to this topic, and FATF reports and statements relating to the ML/TF risks associated with VAs, VA activities, and/or VASPs,[3] for example, highlight and provide further context regarding the ML/TF risks associated with VA activities. While VAs may provide another form of value for conducting ML and TF, and VA activities may serve as another mechanism for the illegal transfer of value or funds, countries should not necessarily categorize VASPs or VA activities as inherently high ML/TF risks. The cross-border nature of, potential enhanced-anonymity associated with, and non-face-to-face business relationships and transactions facilitated by VA activities should nevertheless inform a country's assessment of risk. The extent and quality of a country's regulatory and supervisory framework as well as the implementation of risk-based controls and mitigating measures by VASPs also influence the overall risks and threats associated with covered VA activities. The Guidance also recognizes that despite these measures, there may still be some residual risk, which

---

2 Further information on central bank digital currencies is in Annex B of the FATF's *Report to the G20 on So-called Stablecoins*.

3 See, for example, the July 2018 FATF report to G-20 Finance Ministers and Central Bank Governors; the February 2019 FATF public statement on mitigating risks from virtual assets; ~~and~~ the April 2019 FATF report to G-20 Finance Ministers and Central Bank Governors, the June 2020 12-month review of the revised FATF Standards on virtual assets/VASPs, the June 2020 FATF report to the G20 Finance Ministers and Central Bank Governors on so-called stablecoins and the September 2020 FATF report on virtual assets red flag indicators of ML/TF. ~~,~~

competent authorities and VASPs should consider in devising appropriate solutions. Jurisdictions should individually examine VAs and VASP activities in the context of their own financial sectors and regulatory and supervisory systems to arrive at an assessment of their risk.

19. Since the FATF finalised the revision to its Standards in June 2019, it has continued to monitor trends in the use of VAs for ML/TF purposes. As set out in its September 2020 report on *Virtual Asset Red Flag Indicators of ML/TF,* the FATF has observed that VAs are becoming increasingly mainstream for criminal activity more broadly. The majority of VA-related offences focused on predicate or ML offences. Notwithstanding, criminals did make use of VAs to evade financial sanctions and to raise funds to support terrorism. The types of offences reported by jurisdictions include ML, the sale of controlled substances and other illegal items (including firearms), fraud, tax evasion, computer crimes (e.g. cyberattacks resulting in thefts), child exploitation, human trafficking, sanctions evasion, and TF. Among these, two types of misuse stand out as the most common. These are illicit trafficking in controlled substances, either with sales transacted directly in VAs or the use of VAs as an ML layering technique, and frauds, scams, ransomware, and extortion. More recently, professional ML networks have started exploiting VAs as one of their means to transfer, collect, or layer proceeds.

~~16.~~20. The Guidance recognizes that "new" or innovative technologies or mechanisms for engaging in, or that facilitate financial activity may not automatically constitute "better" approaches and that jurisdictions should also assess the risks arising from and appropriately mitigate the risks such new methods of performing a traditional or already-regulated financial activity, such as the use of VAs in the context of payment services or securities activities, as well.

~~17.~~21. Other stakeholders, including VASPs, FIs and other obliged entities that provide banking or other financial services to VASPs or to customers involved in VA activities ~~or that engage in VASP activities~~ themselves should also consider the aforementioned factors. As with all customers, FIs should apply a risk-based approach when considering establishing or continuing relationships with VASPs or customers involved in VA activities, evaluate the ML/TF risks of the business relationship, and assess whether those risks can be appropriately mitigated and managed (see Section IV). It is important that FIs apply the risk-based approach properly and do not resort to the wholesale termination or exclusion of customer relationships within the VASP sector without an appropriately-targeted ~~a proper~~ risk assessment.

~~18.~~22. In considering the Guidance, countries, VASPs and other obliged entities that engage in or provide covered VA activities should recall the key principles underlying the design and application of the FATF Recommendations and that are relevant in the VA context:

a) *Functional equivalence and objectives-based approach*. The FATF requirements, including as they apply in the VA space, are compatible with a variety of different legal and administrative systems. They broadly explain what must be done but not in an overly-specific manner about how implementation should occur in order to allow for different options, where appropriate. Any clarifications to the requirements should not require jurisdictions that have already adopted adequate measures to achieve the objectives of the FATF Recommendations to change the form or substance of their laws and regulations. The Guidance seeks to support ends-based or objectives-based implementation of the relevant FATF Recommendations rather than impose a rigid prescriptive one-size-fits-all regulatory regime across all jurisdictions.

b) *Technology-neutrality and future-proofing.* The requirements applicable to VAs, as value or funds, to covered VA activities, and to VASPs apply irrespective of the technological platform involved. Equally, the requirements do notare not intended to give preference to specific products, services, or solutions offered by commercial providers, including technological implementation solutions that aim to assist providers in complying with their AML/CFT obligations. Rather, the requirements are intended to have sufficient flexibility so that countries and relevant entities can apply them to existing technologies as well as to evolving and emerging technologies without requiring additional revisions.

c) *Level-playing field (functional treatment).* Countries and their competent authorities should treat all VASPs on an equal footing from a regulatory and supervisory perspective in order to avoid jurisdictional arbitrage. As with FIs and DNFBPs, countries should therefore subject VASPs to AML/CFT requirements that are functionally equivalent to other entities when they offer similar products and services and based on the activities in which the entities engage. Countries and their competent authorities should treat all VASPs, regardless of business model, on an equal footing from a regulatory and supervisory perspective when they provide fundamentally similar services. It is an assessment of risks, based on the nature of the products and services offered, that should guide countries in imposing regulation and supervision. Moreover, all countries should strive to ensure their domestic regimes contribute to even and efficient implementation globally in order to avoid jurisdictional and supervisory arbitrage, although there is no impediment to countries imposing additional requirements that go beyond the FATF Standards to respond to the jurisdictions' own risks or policies. In addition, countries should aim to keep regulation and supervision for VASPs consistent with that which it uses for FIs that provide functionally similar services with similar ML/TF risks. As with FIs and DNFBPs, countries should therefore subject VASPs to AML/CFT requirements that are functionally equivalent to other entities when they offer similar products and services with similar risks and based on the activities in which the entities engage.

2.

19.23. This Guidance is non-binding and does not overrule the purview of national authorities, including on their assessment and categorization of VASPs, VAs, and VA activities, as per the country or regional circumstances, the prevailing ML/TF risks, and other contextual factors. It draws on the experiences of countries and of the private sector and is intended to assist competent authorities, VASPs, and relevant FIs (*e.g.*, banks engaging in covered VA activities) in effectively implementing the FATF Recommendations using a risk-based approach.

Structure

20.24. This Guidance is organized as follows: Section II examines how VA activities and VASPs fall within the scope of the FATF Recommendations; Section III describes the application of the FATF Recommendations to countries and competent authorities; Section IV explains the application of the FATF Recommendations to VASPs and other obliged entities that engage in or provide VA covered activities, including FIs such as banks and securities broker-dealers, among others; and Section V provides examples of jurisdictional approaches to regulating, supervising, and enforcing covered VA activities and VASPs (and other obliged entities) for AML/CFT; and Section VI sets out Principles for International Co-operation and Information-Sharing amongst VASP Supervisors.

21.25. Annex A es A, B, and C include relevant resources that augment this Guidance, including the June 2014 *FATF Virtual Currencies: Key Definitions and Potential AML/CFT Risks* paper, the June 2015 VC Guidance,sets out the updated text of

Recommendation 15 and its Interpretive Note, and the "virtual asset" and "virtual asset service provider" definitions within the FATF Glossary. Annex B sets out the changes made to this Guidance in the June 2021 update.

Section II – Scope of FATF Standards

~~22.~~26. Section II discusses the applicability of the risk-based approach to VA activities and VASPs and explains how these activities and providers should be subject to AML/CFT requirements under the international standards. As described in paragraph 2 of INR. 15, VASPs are subject to the relevant measures under the FATF Recommendations based on the types of activities in which they engage. Similarly, VAs are captured by the relevant measures under the FATF Recommendations that relate to funds or value, broadly, or that specifically reference funds- or value-based terms.

~~23.~~27. It should be underscored that when VASPs engage in traditional fiat-only activities or fiat-to-fiat transactions (which are outside the scope of the virtual-to-virtual and virtual-to-fiat activities covered by the VASP definition), they are ~~of course~~ subject to the same measures as any other equivalent traditional institution or entity normally would be under the FATF standards.

Initial Risk Assessment

~~24.~~28. The FATF Recommendations do not ~~predetermine~~ prejudge any sector as higher risk. The standards identify sectors that may be vulnerable to ML and TF; however the overall risk at a national level should be determined by individual jurisdictions through an assessment of the sector—in this case, the VASP sector~~—at a national level~~. Different entities within a sector may pose a higher or lower risk depending on a variety of factors, including products, services, customers, geography, business models and the strength of the entity's compliance program. Recommendation 1 sets out the scope of the application of the risk-based approach as follows: who should be subject to a country's regime; how those subject to the AML/CFT regime should be supervised or monitored for compliance with the regime; how those subject to the AML/CFT regime should be required to comply; and consideration of the engagement in customer relationships by VASPs and other obliged entities involved in covered VA activities. Further, the FATF does not support the wholesale and indiscriminate termination or restriction of business relationships with a particular sector (*e.g.*, FI relationships with VASPs regardless of their risk profile, where relevant) to avoid, rather than manage, risk in line with the FATF's risk-based approach.

~~25.~~29. ~~The FATF has assessed that ML/TF risks exist in relation to VAs, VA financial activities or operations, and VASPs. Accordingly, u~~Under the risk-based approach and in accordance with paragraph 2 of INR. 15, countries should identify, assess, and understand the ML/TF risks emerging from this space and focus their AML/CFT efforts on potentially higher-risk VAs, covered VA activities, and VASPs. Similarly, countries should require VASPs (as well as other obliged entities that engage in VA financial activities or operations or provide VA products or services) to identify, assess, and take effective action to mitigate their ML/TF risks.

~~26.~~30. A VASP's risk assessment should take into account all of the risk factors that the VASP as well as its competent authorities consider relevant, including the types of services, products, or transactions involved; customer risk; geographical factors; type(s) of VA exchanged, among other factors.

~~27.~~31. VAs can enable non-face-to-face business relationships or permit transactions to take place without the use, involvement or regulatory regime of a VASP or a FI. ~~As with many financial payments methods, for example, VAs can enable non-face-to-face business relationships~~ . Further, VAs can be used to quickly move funds globally, nearly instantaneously and largely irreversibly, and to facilitate a range of financial activities—from money or value transfer services to securities, commodities or derivatives-related activity, among others. Thus, the absence of face-to-face contact or the lack of involvement of a regulated VASP or FI in VA financial activities or operations may indicate higher ML/TF risks, and thus may require appropriate risk mitigating measures to identify or combat relevant illicit activities or frauds, such as the use of strong digital identity solutions.[4] Similarly, VA products or services that facilitate pseudonymous or anonymity-enhanced transactions also pose higher ML/TF risks, particularly if they inhibit a VASP's ability to identify the beneficiary. ~~The latter~~Lack of customer and counterparty identification is especially concerning in the context of VAs, which are cross-border in nature. If customer identification and verification measures do not adequately address the risks associated with non-face-to-face or opaque transactions, the ML/TF risks increase, as does the difficulty in tracing the associated funds and identifying transaction counterparties.

~~28.~~ The extent to which users can use VAs or VASPs globally for making payments or transferring funds is also an important factor that countries should take into account when determining the level of risk. Illicit users of VAs, for example, may take advantage of the global reach and transaction speed that VAs provide, as well as ~~of the~~ inadequate or inconsistent regulation or supervision of VA financial activities and providers across jurisdictions, which creates an inconsistent legal and regulatory playing field in the VA ecosystem. As with other mobile or Internet-based payment services and mechanisms that can be used to transfer funds globally or in a wide geographical area with a large number of counterparties, VAs can be more attractive to criminals for ML/TF purposes than purely domestic business models.

32.

~~29.~~33. In addition, VASPs located in one jurisdiction may offer their products and services to customers located in another jurisdiction where they may be subject to different AML/CFT obligations and oversight. This is of concern where the VASP is located in a jurisdiction with weak or even non-existent AML/CFT controls, or where there is a shortfall in the ability of jurisdictions to provide the widest range of international co-operation. Similarly, the sheer range of providers in the VA space and their presence across several, if not nearly all, jurisdictions can increase the ML/TF risks associated with VAs and VA financial activities due to potential gaps in customer and transaction information. This is a particular concern in the context of cross-border transactions and when there is a lack of clarity on which entities or persons (natural or legal) involved in the transaction are subject to AML/CFT measures and which countries are responsible for regulating (including licensing and/or registering) and supervising or monitoring those entities for compliance with their AML/CFT obligations. Further, if a VA achieves sufficient global adoption by customers such that it is used as a medium of exchange and store of value without the use of a VASP or other regulated financial institution, lack of AML/CFT controls and compliance could pose especially high risk.

Box 1. So-called stablecoins and ML/TF risks

[4] Further information on digital identity is available in the *FATF Guidance on Digital ID*.

So-called stablecoins purport to overcome the price volatility issues associated with VAs by maintaining a stable value relative to some reference asset or assets. They share many of the same potential ML/TF risks as some VAs, because of their potential for anonymity, global reach and use to layer illicit funds. The degree to which these risks materialise depends on the features of the so-called stablecoin arrangement, the extent to which jurisdictions have implemented AML/CFT mitigating measures, and also, critically, on the extent to which there is mass-adoption of the so-called stablecoin.

Some proposed so-called stablecoins have been sponsored by large technology, telecommunications or financial firms and seem to have the potential for rapid scaling and mass-adoption. In the same way as any other large-scale value transfer system, this propensity for mass-adoption significantly increases their risk of criminal abuse for ML/TF purposes. In its report to G20, the FATF considered that so-called stablecoins with potential for mass-adoption are more likely to be centralised to some extent, with an identifiable central developer or governance body. Such central bodies will, in general, be covered by the FATF Standards as either a FI or a VASP. So-called stablecoins may also be decentralized without a clearly identifiable central developer or governance body. While decentralised so-called stablecoins without such an identifiable central body may, on the face of it, carry greater ML/TF risks due to their diffuse operation, the lack of a central body may reduce the likelihood of mass-adoption. It is important that ML/TF risks of so-called stablecoins, particularly those with potential for mass-adoption, are analysed in an ongoing and forward-looking manner and these risks are mitigated before such arrangements are launched.

Importantly, the FATF Standards apply to so-called stablecoins and their service providers either as VAs and VASPs or as traditional financial assets and their service providers. They should never be outside the scope of AML/CFT controls (see 'What is a VASP?' below for further information about what entities have AML/CFT obligations in a so-called stablecoin arrangement).[5]

Peer-to-peer transactions

34. 'Peer-to-peer' (P2P) transactions are VA transfers conducted without the use or involvement of a VASP or other obliged entity, such as VA transfers between two unhosted wallets. P2P transactions are not explicitly subject to AML/CFT obligations under the FATF Recommendations. This is because the FATF Recommendations generally place obligations on intermediaries between individuals and the financial system, rather than on individuals themselves with some exceptions, such as requirements related to targeted financial sanctions. This is similar to the approach taken with physical fiat currency (cash) transactions, although there are inherent differences between VA transfers and physical cash transfers.

35. The FATF recognises that P2P transactions could pose heightened ML/TF risk, as they can potentially be used to avoid the AML/CFT controls imposed on VASPs and obliged entities in the FATF Recommendations. If P2P transactions gain widespread and mainstream traction and are readily used as a means of payment or investment without a VASP or FI,

[5] See the FATF's report to G20 Finance Ministers and Central Bank Governors on so-called stablecoins for further information about the application of the FATF Standards to so-called stablecoins and their ML/TF risks. Further information on so-called stablecoins, their characteristics and broader regulatory and supervisory issues is set out in the Financial Stability Board's 2020 Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Final Report and High-Level Recommendations.

the number and value of transactions not subject to AML/CFT controls could increase and possibly lead to systemic ML/TF vulnerabilities in some jurisdictions. Moreover, full maturity of these protocols that enable P2P transactions could foreshadow a future without financial intermediaries, potentially challenging the effectiveness of the FATF Recommendations. VASPs and other obliged entities should consider whether any VAs or products they plan to launch, or transact with, will enable P2P transactions and, if so, how ML/TF risks should be mitigated. The ML/TF risks are more difficult to address and mitigate once the products are launched, and thus should be addressed in the design or development phase. Similarly, VASPs and other obliged entities should consider the extent to which their customers may engage in, or are involved, in P2P activity. Countries should also consider how ML/TF risks of P2P transactions for some VAs may be mitigated through, for example, blockchain analytics, which may provide greater visibility over P2P transactions.

Risk factors relating to VAs and VASPs

36. There exist ML/TF risks in relation to VAs, VA financial activities or operations, and VASPs. In addition to consulting the previous FATF works on this subject,[6] and the FATF's general guidance on risk assessments,[7] countries and VASPs should consider the following non-exhaustive list of elements, for example, when identifying, assessing, and determining how best to mitigate the risks associated with covered VA activities and the provision of VASP products or services:

Elements relating to VAs

a) The number and the value of VA transfers; the value and price volatility of the VA issued; the market capitalisation of the VA; the value in circulation; the number of jurisdictions of users and the number of users in each jurisdiction; and the market share in payments for a VA in each jurisdiction; the extent to which the VA is used for cross-border payments and remittance;

b) The potential ML/TF risks associated with VAs that are exchanged with/for fiat currency and removed from the traditional financial system and the extent to which VA-based payment channels/platforms interact with, or are connected to fiat-based payment channels/platforms and digital services/platforms;

c) The nature and scope of the VA payment channel or system (*e.g.*, open- versus closed-loop systems or systems intended to facilitate micro-payments or government-to-person/person-to-government payments);

d) The number and value of VA transfers and those relating to illicit activities (*e.g.*, darknet marketplaces, ransomware and hacking) in the following categories; (1) between VASPs/other obliged entities, (2) between VASPs/other obliged entities and non-obliged entities, and (3) between non-obliged entities (i.e. P2P transactions);

e) The technological development and general adoption of use of anonymizing techniques of VA funds transfer and de-anonymizing techniques (*e.g.*, AECs, mixing and tumbling services, the clustering of wallet addresses and risk

6 For example, the 2015 VC Guidance, 2018 FATF Risk, Trends, and Methods Group papers relating to this topic, and FATF statements and reports relating to the ML/TF risks associated with VAs, VA activities, and/or VASPs. Further information on VAs is also available in the FATF's 2020 *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*.

7 For example, the 2013 *National ML/TF Risk Assessment Guidance* and the 2019 *TF Risk Assessment Guidance*.

assessment of wallet addresses using topological patterns of VA funds transfer via blockchain or DLT analytical tools);

f) Exposure to Internet Protocol (IP) anonymizers such as The Onion Router (TOR), the Invisible Internet Project (I2P) and other darknets, which may further obfuscate transactions or activities and inhibit a VASP's ability to know its customers and implement effective AML/CFT measures;

g) The size of the business, the existing customer-base, the stakeholders, and the significance of the cross-border activities of the issuer and/or the central entity governing the arrangement (where this exists);

~~The risks associated with centralised and decentralised VASP business models;~~

Elements relating to VASPs

a) The number and types of VASPs that are based in a jurisdiction and/or offerings services to customers based in a jurisdiction and the number and amount of transactions relating to each service;

b) The sophistication of the VASP's AML/CFT program, including the existence or absence of appropriate oversight tools to monitor VA and/or VASP activities, including whether there is appropriate knowledge and expertise of the individuals responsible for compliance with the AML/CFT program related to the VA;

c) The size and type of the customer base of the VASP, including the VASP's access to data on its customers and their activity, both within the VASP and if there is potential aggregation across platforms;

d) The nature and scope of the VA account, product or service (*e.g.*, small value savings and storage accounts that primarily enable financially-excluded customers to store limited value) that the VASP offers;

e) Any parameters or measures in place that may potentially lower the provider's (whether a VASP or other obliged entity that engages in VA activities or provides VA products and services) exposure to risk (*e.g.*, limitations on transactions or account balance);

f) The specific business model of the VASP; ~~and~~ whether that business model introduces or exacerbates specific risks and the business, organizational and operational complexity of the VASP;

Whether the VASP operates entirely online (*e.g.*, platform-based exchanges) or in person (*e.g.*, trading platforms that facilitate ~~peer to peer exchanges~~transactions between individual users or kiosk-based exchanges);

g) The potential ML/TF and sanctions risks associated with a VASP's connections and links to jurisdictions;

h) Whether the VASP implements the 'travel rule' or not (see Recommendation 16 in Sections III and IV);

i) Transactions from / to non-obliged entities (meaning e.g. unhosted wallets, apps etc.) and transactions where at an earlier stage P2P transactions have occurred;

j) The specific types of VAs that the VASP offers or plans to offer and any unique features of each VA, such as –AECs, embedded mixers or tumblers, or other products and services that may present higher risks by potentially obfuscating the

transactions or undermining a VASP's ability to know its customers and implement effective customer due diligence (CDD) and other AML/CFT measures;

k) VASPs' interaction with, or management of, any smart contracts[8] that may be used to conduct transactions.

~~30. The potentially higher risks associated both with VAs that move value into and out of fiat currency and the traditional financial system and with virtual-to-virtual transactions;~~

~~31.~~ 1. ~~The risks associated with centralised and decentralised VASP business models;~~

~~32.~~

~~33. The specific types of VAs that the VASP offers or plans to offer and any unique features of each VA, such as AECs, embedded mixers or tumblers, or other products and services that may present higher risks by potentially obfuscating the transactions or undermining a VASP's ability to know its customers and implement effective customer due diligence (CDD) and other AML/CFT measures;~~

~~34. The specific business model of the VASP and whether that business model introduces or exacerbates specific risks;~~

~~35. Whether the VASP operates entirely online (e.g., platform-based exchanges) or in person (e.g., trading platforms that facilitate peer-to-peer exchanges or kiosk-based exchanges);~~

~~36. Exposure to Internet Protocol (IP) anonymizers such as The Onion Router (TOR) or Invisible Internet Project (I2P), which may further obfuscate transactions or activities and inhibit a VASP's ability to know its customers and implement effective AML/CFT measures;~~

~~37. The potential ML/TF risks associated with a VASP's connections and links to several jurisdictions;~~

~~38. The nature and scope of the VA account, product, or service (e.g., small value savings and storage accounts that primarily enable financially-excluded customers to store limited value);~~

~~39. The nature and scope of the VA payment channel or system (e.g., open- versus closed-loop systems or systems intended to facilitate micro-payments or government-to-person/person-to-government payments); as well as~~

~~40. Any parameters or measures in place that may potentially lower the provider's (whether a VASP or other obliged entity that engages in VA activities or provides VA products and services) exposure to risk (e.g., limitations on transactions or account balance).~~

Prohibition or limitation of VAs/VASPs

~~41.~~ 37. Some countries may decide to prohibit or limit VA activities or VASPs, and those VA activities carried out by non-obliged entities, based on their assessment of risk and national regulatory context or in order to support other policy goals not addressed in this Guidance (*e.g.*, consumer or investor protection, market protection, safety and soundness,

[8] In a VA context, a smart contract is a computer program or a protocol that is designed to automatically execute specific actions such as VA transfer between participants without the direct involvement of a third party when certain conditions are met.

or monetary policy). In such cases, some of the specific requirements of R. 15 would not apply, but jurisdictions would still need to assess the risks associated with covered VA activities or providers and have tools and authorities in place to take action for non-compliance with the prohibition or limitation (see sub-section 3.1.1.).

FATF Definitions and Features of the VASP Sector Relevant for AML/CFT

42.38. The FATF Recommendations require all jurisdictions to impose specified AML/CFT requirements on FIs, ~~and~~ DNFBPs and VASPs and ensure their compliance with those obligations. In the Glossary, the FATF defines:

a) "Financial institution" as any natural or legal person who conducts as a business one or more of several specified activities or operations for or on behalf of a customer;

b) "Virtual asset" as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations; and

c) "Virtual asset service provider" as any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

i. Exchange between virtual assets and fiat currencies;

ii. Exchange between one or more forms of virtual assets;

iii. Transfer[9] of virtual assets; and

iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;

v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Background and general considerations for the definition of VA and VASP

39. The purpose of adding the new definitions of VA and VASP to the FATF Glossary was to broaden the applicability of the FATF Recommendations to encompass new types of digital assets and providers of certain services in those assets. It was not intended to subtract from the existing definitions of "funds", "funds or other assets", or from the scope of the various financial services included under the definition of a "financial institution" in the FATF Standards. Many of these terms are not defined and should be interpreted broadly, in accordance with their risk context. Hence, if a country determines that a digital asset falls out of the definition of a VA but is a financial asset, that asset is still covered by the FATF Recommendations as a traditional financial asset. Therefore, the provider of relevant services with that asset may be deemed as a FI.

43.40. Assets should not be deemed uncovered by the FATF Recommendations because of the format in which they are offered and no asset should be interpreted as falling entirely outside the FATF Standards. Each country must determine whether such assets and their activity fall into the definition of VA or traditional financial assets and VASPs or FIs,

[9] 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.

Regardless, the FATF Recommendations apply similarly with only minor accommodations. [10] When deciding how to define VAs in national law or which framework to apply to a given product or provider, countries should consider whether their respective existing AML/CFT regimes are suitable to handle the risks emanating from digital assets. That is, jurisdictions should ensure that digital products and services which do not qualify as VA and VASPs are adequately covered by the frameworks under which they will fall instead and adjust their national law or regulations as needed if not.

Box 2. How the FATF Standards apply to a new asset

New digital token

↓

1. Does the new digital token meet the criteria of a traditional financial asset in a country?

- (a) Does it meet the definition of a security, commodity, derivative or other traditional financial asset under the country's law?
  - Yes – go to 1(b)
  - No – Go to 2
- (b) Is the country's AML/CFT regime for the traditional financial asset suitable for addressing the ML/TF risks associated with the asset?
  - Yes – the asset is regulated as a traditional financial asset
  - No – the country should consider adjusting their national laws or regulations to be suitable *or* consider regulating the asset as a VA (go to 2)

2, As the new digital token is not defined as a traditional financial asset under the country's laws, does the new digital token meet the FATF definition of a VA?

- Yes – the token is regulated as a VA
- No – the token is not covered by the FATF Standards[11]

NB: Depending on how a country has implemented the FATF Standards into their national law, a digital token may be categorised differently in different jurisdictions.

What is a virtual asset?

41. The definition of VA is meant to be interpreted broadly, with jurisdictions relying on the fundamental concepts contained in it to take a functional approach that can accommodate technological advancements and innovative business models. In line with the overall ethos of the FATF Recommendations, these definitions aim for technology neutrality. That is,

[10] These are in relation to customer due diligence (Recommendation 10) and wire transfer rules (Recommendation 16) (i.e. the travel rule). See Sections III and IV below for further explanation of these obligations.

[11] For example. this could might include airline miles, credit card awards, or similar loyalty program rewards or points, which an individual cannot sell onward in a secondary market outside of the closed-loop system

they should be applied based on the basic characteristics of the asset, not the technology it employs. There are therefore a few key elements to elaborate.

42. Firstly, VAs must be digital, and must themselves be digitally traded or transferred and be capable of being used for payment or investment purposes. That is, they cannot be merely digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations, without an inherent ability themselves to be electronically traded or transferred and the possibility to be used for payment or investment purposes.

43. For this reason, a bank record maintained in digital format, for instance, which represents a customer's ownership of fiat currency is not a VA. If it functions as a mere declarative record of ownership or positions in a traditional financial asset that is already covered by the FATF Standards, it is not a VA. However, a digital asset that is exchangeable for another asset, such as a so-called stablecoin that is exchangeable for a fiat currency or a VA at a stable rate, could still qualify as a VA. The key question in this context is whether the VA has inherent value to be traded or transferred and used for payment or investment or, rather, is simply a means of recording or representing ownership of something else. It bears repeating, however, that assets that do not qualify as VAs should not be presumed to fall outside the scope of the FATF Standards. Instead, they may fall under other kinds of traditional financial assets, such as securities, commodities, derivatives or fiat currency. In choosing the terms "traded" and "transferred" the FATF intentionally created a broad, general definition and these terms include the concept of issuance, which could allow multiple limbs of the VASP definition to overlap the same activity. A VA offers the capability to change ownership or the entity entitled to its value. This could include issuing the asset, exchanging it for something else, transferring it to someone else, confiscating or freezing it, or destroying it.

44. The FATF does not intend for an asset to be both a VA and a traditional financial asset at the same time. There may however be instances where the same asset will be classified differently under different national frameworks or the same asset might be regulated under multiple different categorizations. In cases where a jurisdiction determines that an instrument should qualify as a traditional financial asset, authorities should consider whether the existing regime governing traditional financial assets of that type can be appropriately applied to the new digital assets in question (*e.g.,* if the asset in question is the functional digital equivalent of cash, a bearer negotiable instrument or bearer share, how would the mitigation measures in this respect be applied to it).

45. In instances where characterization proves difficult, jurisdictions should assess their regulatory systems and decide which designation will best suit in mitigating and managing the risk of the product. Jurisdictions should also consider the commonly accepted usage of the asset (*e.g.,* whether it used for payment or investment purposes) and what type of asset offers the best fit. Should a jurisdiction choose to define an asset as a traditional financial asset as opposed to a VA, existing AML/CFT standards and the guidance that accompanies traditional financial assets would apply. Consistent with the technology-neutral approach, a blockchain-based asset that is defined as a traditional financial asset would likely not fall under this VA-focused Guidance because the technology used is not the deciding factor in determining which FATF Recommendations apply. Elements of this Guidance may, however, still prove helpful to jurisdictions and the private sector and should supplement other existing guidance in the context of the risk-based approach. Nonetheless, every asset for payment or investment should be subject to obligations applicable either as a VA or a traditional financial asset.

46. The FATF reaffirms previous statements that a so-called stablecoin is covered by the Standards as a VA or as traditional financial asset (*e.g.,* a security) according to the same

criteria used for any other kind of digital asset, depending on its exact nature and the regulatory regime in a country.[12]

What is a VASP?

47. As stated in the FATF Glossary, a "virtual asset service provider" is any *natural or legal person* who is *not covered elsewhere under the Recommendations* and *as a business* conducts one or more of the following activities or operations *for or on behalf of another natural or legal person*:

    i. *Exchange* between virtual assets and fiat currencies;

    ii. *Exchange* between one or more forms of virtual assets;

    iii. *Transfer*[13] 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.

48. As with the definition of VA, the definition of VASP should be read broadly. Countries should take a functional approach and apply the following concepts underlying the definition to determine whether an entity is undertaking the functions of a VASP. Countries should not apply their definition based on the nomenclature or terminology which the entity adopts to describe itself or the technology it employs for its activities. As set out above, the definitions do not depend on the technology employed by the service provider. The obligations in the FATF Standards stem from the underlying financial services offered without regard to an entity's operational model, technological tools, ledger design, or any other operating feature. To assist in illustrating the concepts of the definition, the section below includes examples which use general terms to describe common business models. However, these should not obscure the fact that the definition is meant to be applied based on an assessment of whether the entity in question provides a qualifying service, not these terms themselves.

49. Before looking at individual functions, there are a few common elements that must be understood. As discussed in the VA definition, to avoid repetition or overlap, the definition of VASP only applies to entities "*not covered elsewhere under the Recommendations"*. It excludes other types of FIs or intermediaries covered elsewhere in the FATF Standards. Jurisdictions have to apply the definition that is the most appropriate, based on an understanding of the conceptual foundations of each definition. The primary difference between VASPs and traditional FIs from the standpoint of this Guidance, as discussed above, is the application of Recommendations 10 and 16, so jurisdictions may wish to apply the definition that provides more thorough regulatory and supervisory coverage.[14]

---

12 The FATF considers that the term "stablecoin" is not a distinct legal or regulatory classification for a type of asset, and is instead primarily a marketing term. In order to avoid unintentionally endorsing their claims, this document therefore refers to them as 'so-called stablecoins. See the FATF's report to G20 Finance Ministers and Central Bank Governors on so-called stablecoins for further information.

13 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.

14 These are in relation to customer due diligence (Recommendation 10), to lower the CDD occasional transaction threshold, and wire transfer rules (Recommendation 16) which apply in an amended way to VA transfers (i.e. the travel rule). See Sections III and IV below for further explanation of these obligations.

50. The word "*person*" in the definition refers to the entity that provides the capability, offers the service, or facilitates the transaction. The person can be either a legal person, such as a company, or a natural (individual) person.

51. The phrase "*as a business*" is meant to separate those who may carry out a function on a very infrequent basis for non-commercial reasons from VASPs. To satisfy this portion of a definition, the entity must carry out this function on behalf of another natural or legal person as opposed to on behalf of itself, for commercial reasons, and must do so on at least a sufficiently regular basis, rather than infrequently. The VASP will have customer due diligence obligations at the time of on-boarding and on an ongoing basis in relation to the customer.

52. A person who meets these requirements will then be a VASP if it carries out one or more of the five categories of *activity or operation* described in the VASP definition (*i.e.*, "exchange" of virtual/fiat, "exchange" of virtual/virtual, "transfer," "safekeeping and/or administration," and "participation in and provision of financial services related to an issuer's offer and/or sale"). The coverage of each limb of the definition is set out below.

Exchange and transfer

53. The first limb of the definition of VASP refers to any service in which VAs can be given in exchange for fiat currency or vice versa. If parties can pay for VAs using fiat currency or can pay using VAs for fiat currency, the offerer, provider, or facilitator of this service when acting as a business is a VASP. Similarly, in limb (ii), if parties can use one kind of VA as means of exchange or form of payment for another VA, the offerer, provider or facilitator of this service when acting as a business is a VASP. It should be emphasized that limbs (i) and (ii) include the above activities, regardless of the role the service provider plays vis-à-vis its customers as a principal, as a central counterparty for clearing or settling transactions, as an executing facility or as another intermediary facilitating the transaction. A VASP does not have to provide every element of the exchange or transfer in order to qualify as a VASP, so long as it undertakes the exchange activity as a business on behalf of another natural or legal person.

54. Limb (iii) in the definition of VASP covers any service allowing users to transfer ownership, or control of a VA to another user. The FATF Standards define this to mean "conduct[ing] a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another." To help illustrate what this limb covers in practice, it is useful to consider the current nature of the VA. If a new party has custody or ownership of the VA, has the ability to pass control of the VA to others, or has the ability to benefit from its use, then transfer has likely occurred. This control does not have to be unilateral and multisignature[15] processes are not exempt (see limb (iv) below), where a VASP undertakes the activity as a business on behalf of another natural or legal person.

55. Where custodians need keys held by others to carry out transactions, these custodians still have control of the asset. A user, for example, who owns a VA, but cannot send it without the participation of others in a multisignature transaction, likely still controls it for the purposes of this definition. Service providers who cannot complete transactions without a key held by another party are not disqualified from falling under the definition of a VASP, regardless of the numbers, controlling power and any other properties of the involved

[15] In a multisignature process or model, a person needs several digital signatures (and therefore several private keys) to perform a transaction from a wallet.

parties of the signature. The limb is conceptually similar to what Recommendation 14 on money and value transfer services (MVTS) covers for traditional financial assets. An example of a service covered by (iii) includes the function of facilitating or allowing users to send VAs to other individuals, as in a personal remittance payment, payment for non-financial goods or services, or payment of wages. A provider offering such a service will likely be a VASP.

56. Exchange or transfer services may also occur through so-called decentralized exchanges or platforms. "Decentralized or distributed application (DApp)," for example, is a term that refers to a software program that operates on a P2P network of computers running a blockchain protocol—a type of distributed public ledger that allows the development of other applications. These applications or platforms are often run on a distributed ledger but still usually have a central party with some measure of involvement, such as creating and launching an asset, setting parameters, holding an administrative "key" or collecting fees. Often, a DApp user must pay a fee to the DApp, which is commonly paid in VAs, for the ultimate benefit of the owner/operator/developer/community in order to develop/run/maintain the software. DApps can facilitate or conduct the exchange or transfer of VAs.

57. A DApp itself (i.e. the software program) is not a VASP under the FATF standards, as the Standards do not apply to underlying software or technology (see below). However, entities involved with the DApp may be VASPs under the FATF definition. For example, the owner/operator(s) of the DApp likely fall under the definition of a VASP, as they are conducting the exchange or transfer of VAs as a business on behalf of a customer. The owner/operator is likely to be a VASP, even if other parties play a role in the service or portions of the process are automated. Likewise, a person that conducts business development for a DApp may be a VASP when they engage as a business in facilitating or conducting the activities previously described on behalf of another natural or legal person. The decentralization of any individual element of operations does not eliminate VASP coverage if the elements of any part of the VASP definition remain in place.

58. Other common VA services or business models may also constitute exchange or transfer activities based on items (i), (ii), and (iii) of the VASP definition, and the natural or legal persons behind such services or models would therefore be VASPs if they conduct or facilitate the activity as a business on behalf of another person. These can include:

    a) VA escrow services, including services involving smart contract technology, that VA buyers use to send or transfer fiat currency in exchange for VAs, when the entity providing the service has custody over the funds;

    b) brokerage services that facilitate the issuance and trading of VAs on behalf of a natural or legal person's customers;

    c) order-book exchange services, which bring together orders for buyers and sellers, typically by enabling users to find counterparties, discover prices, and trade, potentially through the use of a matching engine that matches the buy and sell orders from users (although a platform which is a pure-matching service for buyers and sellers of VAs and does not undertake any of the services in the definition of a VASP would not be a VASP); and

    d) advanced trading services, which may allow users to access more sophisticated trading techniques, such as trading on margin or algorithm-based trading.

59. Exchange and/or transfer business models can include VA exchanges or VA transfer services that facilitate the exchange of VA for real currency and/or other forms of VA for remuneration (*e.g.,* for a fee, commission, spread, or other benefit). These models typically

accept a wide range of payment methods, including cash, wires, credit cards, and VAs. Traditional VA exchange or transfer services can be administrator-affiliated, non-affiliated, or a third-party provider. Providers of kiosks—often called "ATMs," bitcoin teller machines," "bitcoin ATMs," or "vending machines"—may also fall into the above definitions because they provide or facilitate covered VA activities via physical electronic terminals (the kiosks) that enable the owner/operator to facilitate the exchange of VAs for fiat currency or other VAs and/or the exchange of fiat currency for VAs.

Safekeeping and/or administration[16]

60. Limb (iv) of the VASP definition should also be read expansively. Any entity that provides or facilitates control of assets or governs their use may qualify under part (iv) as this is the conceptual meaning of the words "administration" and "safekeeping". In simplest terms, "safekeeping" consists of the service of holding a VA or the private keys to the VA on behalf of a customer. As in the definition of "transfer", this would include circumstances where keys or credentials held by others are required in order to change the assets disposition, such as multisignature processes. In order to further clarify, "administration" could also include the concept of "management."

61. The term "control" should be understood as the ability to hold, trade, transfer, spend or destroy the VA. Parties that can use a VA or change its disposition have control of it. This does not mean the control must be unilateral, and the existence of a multi-signature model or models in which multiple parties must use keys for a transaction to happen does not mean a particular entity does not maintain control.

62. This limb of the definition would include, for example, most custodial wallet service providers because they hold and/or keep VAs on behalf of customers. Those who may offer escrow services, such as lawyers, should consider whether they provide this service routinely as a business and whether the elements of control are actually offered by themselves or by a party to whom they outsource the control, such as a custodial wallet service provider to which they consign the VAs. Providing the functions outlined in the definition should be the determining factor rather than a categorization as a lawyer. When in doubt, the plain language of the definitions should be interpreted flexibly to encompass any provider that helps/promotes customers hold or use their VAs or runs the functioning of the VA ecosystem itself. The explanation of "control" provided above holds for the discussion of "enabling control" in this section as well.

63. In the context of limb (iv) of the VASP definition, countries should account for services or business models that provide the function of safeguarding the value of a customer's VAs or the power to manage or transfer the VAs, under the assumption that such management and transmission will only be done according to the owner's/customer's instructions. Safekeeping and administration services could include persons that have control of the private key associated with VAs belonging to another person or control of smart contracts to which they are not a party that involve VAs belonging to another person.

Financial services related to an issuer's offer and/or sale

64. With respect to limb (v) of the VASP definition, this element of the definition includes financial services provided by the issuer of a VA as well as services provided by a VASP

16 The terminology used in this section (such as "safekeeping", "administration" and "ancillary services") are used and interpreted in the context of VAs/VASPs. They should not confused with the usage of such terms in other situations (e.g. in relation to banking and other traditional financial instruments or services).

affiliated or unaffiliated with the issuer in the context of issuance, offer, sale, distribution, ongoing market circulation and trading of a VA (*e.g.,* including book building, underwriting, market making, etc.). However, the licensor of a software may not, absent further involvement, be covered by limb (v). By contrast, an entity that provides software to facilitate an issuance and performs any service identified above on VAs, such as procuring purchasers for the VA, or other financial services, may be covered by this limb.

65. Natural or legal persons that facilitate the issuance, offer, sale, distribution, ongoing market circulation and trading of VAs, including by accepting purchase orders and funds and purchasing VAs from an issuer to resell and distribute the funds or assets, may also fall within the scope of limbs (i)-(iv) of the VASP definition. For example, ICOs are generally a means to raise funds for new projects from early backers and the natural and legal persons facilitating the issuance may provide services that involve exchange or transfer activity as well as issuance offer and/or sale activity.

66. A jurisdiction's applicable AML/CFT obligations governing service providers that participate in or provide financial services relating to an issuer's issuance, offer, sale and/or distribution, such as in the context of ICOs, may therefore involve both the jurisdiction's money transmission regulations as well as its regulations governing securities, commodities, or derivatives activities.

Box 3. Example of characteristics of initial coin offerings (ICOs)

Digital assets can be issued and/or transferred using distributed ledger or blockchain technology. One mechanism for distributing such assets is through an event commonly referred to as an ICO. In an ICO, an issuer or promoter typically offers a digital asset for sale in exchange for fiat currency or another VA. ICOs typically are announced and promoted online through various marketing materials. Issuers or promoters often release a "white paper" describing the project and promoting the ICO. Issuers or promoters may tell prospective purchasers that the capital raised from the sales will be used to fund development of a digital platform, software, or other projects and that, at some point, the digital asset may be itself be used to access the platform, use the software, or otherwise participate in the project. During the offering, issuers or promoters may lead purchasers of the digital asset to expect a return on their investment or to participate in a share of the returns provided by the project. After they are issued, the digital assets may be resold to others in a secondary market (*e.g.,* on digital asset trading platforms or through VASPs).

In determining how the definition of VASP applies to entities in an ICO, it is the facts and circumstances underlying an asset, activity or service that will determine the categorization, rather than any labels or terminology used by market participants. For example, a person creates a digital asset that meets the definition of a VA. The person sells the VA to purchasers, even though the VA itself is to be delivered to the purchaser at a later date and the business uses the value received from the sale to develop the platform or ecosystem in which the VA eventually may be used. In this scenario, the person selling the VA is a VASP, as it provides financial services related to the issuance of the VA (limb (v) of the VASP definition) to customers. Any business which assists the person provides additional financial services related to the offer and/or sale of the VA, regardless of whether they are formally affiliated with the person, would also be a VASP under limb (v) of the VASP definition. It does not matter whether the customer intends to use the VA as an investment or as means of payment.

Alternatively, the digital asset in the above example may be considered to be a security under the laws of a country. In this circumstance, the asset would be regulated as a security the issuer of promoter of the ICO would be regulated as a FI under a country's securities laws (see Box 1). Therefore, whether the issuer of the digital asset will be considered a VASP or an issuer of securities will depend on the unique facts and circumstances of the ICO and the laws of the country. Other jurisdictions may also have a different approach which may include payment tokens. A person may be engaged in activity that may subject them to more than one type of regulatory framework, and the digital assets used by such person may similarly be subject to more than one type of regulatory framework.

Scope of the definition

67. Despite the many and frequently changing marketing terms and innovative business models developed in this sector, the FATF envisions very few VA arrangements will form and operate without a VASP involved at some stage if countries apply the definition correctly.

68. As previously stated, the FATF Standards are intended to be technology neutral. As such, the FATF does not seek to regulate the technology that underlies VAs or VASP activities, but rather the natural or legal persons behind such technology or software applications that facilitate financial activity or conduct as a business the aforementioned VA activities on behalf of another natural or legal person. A person that develops or sells either a software application or a VA platform (*i.e.,* a software developer) may therefore not constitute a VASP when solely developing or selling the application or platform. They may however be a VASP if they also use the new application or platform to engage as a business in exchanging or transferring funds or conducting any of the other financial activity described above on behalf of another natural or legal person. Moreover, a party directing the creation and development of the software or platform and launching it for them to provide financial services for profit likely qualifies as a VASP, and is therefore responsible for complying with the relevant AML/CFT obligations. It is the provision of financial services associated with that software application or platform, and not the writing or development of the software itself, which is in scope of the VASP definition.

69. The FATF also does not seek to regulate as VASPs natural or legal persons that provide ancillary services or products to a VA network. This includes the provision of ancillary services to hardware wallet manufacturers or to non-custodial wallets, to the extent that they do not also engage in or facilitate as a business any of the aforementioned covered VA activities or operations on behalf of their customers. Likewise, natural or legal persons that solely engage in the operation of a VA network and do not engage in or facilitate any of the activities or operations of a VASP on behalf of their customers (*e.g.,* internet service providers that offer the network infrastructure, cloud service providers that offer the computing resources, and miners and validators that validate, create and broadcast blocks of transactions) are not VASPs under the FATF Standards, even if they conduct those activities as a business. Individual jurisdictions however may choose to extend their AML/CFT regimes to include them as regulated entities. Furthermore, companies affiliated with VASPs, which facilitate financial activities or conduct as a business the aforementioned VA activities, should be considered as VASPs".

70. Just as the FATF does not seek to regulate the individual users (not acting as a business) of VAs as VASPs—though recognizing that such users may still be subject to compliance obligations under a jurisdiction's sanctions or enforcement framework—the FATF similarly does not seek to capture the types of closed-loop items that are non-transferable, non-exchangeable, and non-fungible. Such items might include airline miles, credit card awards, or similar loyalty program rewards or points, which an individual cannot sell

onward in a secondary market outside of the closed-loop system. Rather, the VA and VASP definitions are intended to capture specific financial activities and operations (*i.e.,* transfer, exchange, safekeeping and administration, issuance, etc.) and assets that are convertible or interchangeable—whether virtual-to-virtual, virtual-to-fiat or fiat-to-virtual. The acceptance of VAs as payment for goods and services, as in the acceptance of VA by a merchant when effecting purchase of goods, for instance, also does not constitute a VASP activity. A service that facilitates companies accepting VA as payment would, however, be a VASP.

71. Conversely, AML/CFT regulations will apply to covered VA activities and VASPs, regardless of the type of VA involved in the financial activity (*e.g.*, a VASP that uses or offers AECs to its customers for various financial transactions), the underlying technology, or the additional services that the platform potentially incorporates (such as a mixer or tumbler or other potential features for obfuscation).

72. For so-called stablecoins, a range of the entities involved in any so-called stablecoin arrangement will have AML/CFT obligations under the revised FATF Standards. So-called stablecoins may have a central developer or governance body. A governance body consists of one or more natural or legal persons who establish or participate in the establishment of the rules governing the stablecoin arrangement (*e.g.*, determine the functions of the so-called stablecoin, who can access the arrangement and whether AML/CFT preventive measures are built into the arrangement). They may also carry out the basic functions of the stablecoin arrangement (such as managing the stabilization function) or this may be delegated to other entities. They may also manage the integration of the so-called stablecoin into telecommunications platforms or promote adherence to common rules across the stablecoin arrangement. Each natural or legal person constituting the governance body could also be a VASP depending on the extent of the influence it may have.

~~44.~~73. Where such a central body exists, they will, in general, be covered by the FATF Standards either as a FI (e.g., as a business involved in the 'issuing and managing means of payment') or a VASP (e.g. under limb (v) of the VASP definition) and can be held accountable for AML/CFT controls across the arrangement and taking steps to mitigate ML/TF risks.[17] This is particularly the case if the governance body carries out multiple functions in the so-called stablecoin arrangement (such as managing the stabilisation function). If one or more parties have decision-making authority over structures that affect the inherent value of a VA, such as changing reserve requirements or monetary supply for a so-called stablecoin, they are likely to be VASPs as well, depending on the extent of the influence each party has. Again, this is not meant to implicate those developing software code, but rather the decision-making entity that controls the terms of the financial service provided. While not determinative on its own, another potential financial indicator for determining who the VASP is in a given set of circumstances is the party that profits from the use of a VA. A range of other entities in the so-called stablecoin arrangement may also have AML/CFT obligations, such as exchanges or custodial wallet services. To demonstrate this, a hypothetical case study is set out in Box 4. It is important to note that the exact details of any arrangement must receive independent scrutiny to make these determinations.[18]

---

17 This is also consistent with the case of "New payment products and services (NPSS)" providers in the FATF's report on prepaid cards, mobile payments and internet-based payment services for further information: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

18 Further detail on the application of the FATF Standards to different entities in a so-called stablecoin arrangement is set out in the FATF's G20 report on so-called stablecoins for further information.

Box 4. Hypothetical case study of a so-called stablecoin arrangement and the application of the FATF Standards

Scenario[19]

A company ("**Company**") is designing a DLT-based platform to issue a digital asset that is intended to act as a so-called stablecoin ("**Coin**").

The Coin will be backed by assets that are held in accounts at a number of global FIs (collectively, the "**Reserve Fund**"), that is managed by the Company. The Coin's market value will be maintained in line with the value of the assets held in the Reserve Fund through the **Authorised Participant** mechanism. Only Authorised Participants will be able to purchase or redeem Coins from the Reserve Fund through the Company. Under the Company's proposed ecosystem, the Company and third parties (collectively, the "**Validators**") will operate a permissioned blockchain network using other third parties' cloud infrastructure.

The Company, third parties and individual users will be able to access, use and transact with the Coin. To connect to the network, any third parties, such as trading platforms and custodial wallet providers, will need to obtain approval from the Company. Coin wallets will permit users to send, receive and store the Coin, and any developers/third parties can offer their customized wallets. Coins will be transferred following the rules defined by the Company and assessed by regulators before commencing operation. Merchants will also be able to use the Coin as payment for goods and services.

Obliged Entities and their AML/CFT obligations under the FATF Standards.

The Company is a VASP under the FATF Standards as its functions include administering the Coin and issuing/redeeming of the Coin, which fall under the scope of limbs (iv) and (v) of the definition of VASP respectively. The Company will have AML/CFT obligations in addition to those of other third-parties with AML/CFT obligations in the ecosystem. Under the FATF Standards, the Company can be held accountable for the implementation of AML/CFT controls across the ecosystem (e.g. in the design of the Coin).

Authorised Participants are also VASPs as their function includes facilitating the issuance, distribution, and trading of VAs which falls under limb (v) of the definition of VASP. Trading platforms are VASPs as their functions include exchanging between the Coins and fiat currencies, transferring Coins, and safekeeping and/or administration of the Coins, which fall under the scope of limb (i), (iii) and (iv) of the VASP definition. Custodial wallet providers are VASPs as their functions include transferring Coins and safekeeping and/or administration of Coins, which fall under the scope of limb (iii) and (iv) of the VASP definition. Developers are VASPs if they deploy programs whose functions fall under the definition of VASP and they deploy those programs as a business on behalf of customers.

19 The scenario included in this case study is adapted from the case study included in IOSCO's March 2020 report on *Global Stablecoin Initiatives*. It has been amended to fit the AML/CFT context.

Participants in the ecosystem who do not fall under the definition of VASPs in the FATF Standards include; the global FIs whose functions are only managing the Reserve Fund (although they are covered under the FATF Standards as FIs); Validators, except for the Company, whose functions are only validating transactions; cloud service providers whose functions are only offering the operation of infrastructure; manufactures of hardware wallets whose functions are only manufacturing and selling the devices; software providers of unhosted wallets whose functions are only developing and selling the software; merchants which are only providing goods and services in exchange for Coins; and individual users.

It is important to note that the exact details of any arrangement must receive prior adequate and independent scrutiny to make these determinations and the exact application of AML/CFT measures will depend on each individual country. Depending on the individual country, laws relating to traditional financial assets such as securities, commodities and derivatives may be implicated in this scenario as well. Countries can also adopt other measures if they consider the ML/TF risks are unacceptably high, such as in relation to potential P2P transactions (see Section III for further information on what measures countries could take).

74. Some platforms and providers offer the ability to conduct VA transfers directly between individual users. For platforms and services offering VA transfers between individual users as for all other service providers, the broad reading of the definitions above will decide whether parties to providing such a service are VASPs on a functional basis, not on the basis of self-description or technology employed. Only entities that provide very limited functionality falling short of exchange, transfer, safekeeping, administration, control, and issuance will generally not be a VASP. For example, this may include websites which offer only a forum for buyers and sellers to identify and communicate with each other without offering, even in part, those services which are included in the definition of VASP.

75. For self-described P2P platforms, jurisdictions should focus on the underlying activity, not the label or business model. Where the platform facilitates the exchange, transfer, safekeeping or other financial activity involving VAs (as described in limbs (i)-(v) of the VASP definition), then the platform is necessarily a VASP conducting exchange and/or transfer activity as a business on behalf of its customers. Launching a service as a business that offers a qualifying function, such as transfer of assets, may qualify an entity as a VASP even if that entity gives up control after launching it, consistent with the discussion of the lifecycle of VASPs below. Some kinds of "matching" or "finding" services may also qualify as VASPs even if not interposed in the transaction. The FATF takes an expansive view of the definitions of VA and VASP and considers most arrangements currently in operation, even if they self-categorize as P2P platforms, may have at least some party involved at some stage of the product's development and launch that constitutes a VASP. Automating a process that has been designed to provide covered services does not relieve the controlling party of obligations.

76. The expansiveness of these definitions represents a conscious choice by the FATF. Despite changing terminology and innovative business models developed in this sector, the FATF envisions very few VA arrangements will form and operate without a VASP involved at some stage. Where customers can access a financial service, it stands to reason that some party has provided that financial service, even if the act of providing it was temporary or shared among multiple parties. Jurisdictions should take particular care to assess any claims that businesses may make as to models of decentralization or distributed services, and conduct their own assessment of the business model in line with its risk and their ability to mitigate these risks.

77. The FATF recognises however that such an approach can bring practical challenges to competent authorities in identifying which entities are VASPs and defining their regulatory perimeter. When there is a need to assess a particular entity to determine whether it is a VASP or evaluate a business model where VASP status is unclear, a few general questions can help guide the answer. Among these would be who profits from the use of the service or asset, who established and can change the rules, who can make decisions affecting operations, who generated and drove the creation and launch of a product or service, who possesses and controls the data on its operations, and who could shut down the product or service. Individual situations will vary and this list offers only some examples.

78. Flexibility is particularly relevant in the context of VAs and VA activities, which involve a range of products and services in a rapidly-evolving space. Some items—or tokens—that on their face do not appear to constitute VAs may in fact be VAs that enable the transfer or exchange of value or facilitate ML/TF. Secondary markets also exist in both the securities and commodities sectors for "goods and services" that are fungible and transferable. For example, users can develop and purchase certain virtual items that act as a store of value and in fact accrue value or worth and that can be sold for value in the VA space.

79. The determination of whether a service provider meets the definition of a VASP should take into account the lifecycle of products and services. Launching a service that will provide VASP services, for instance, does not relieve a provider of VASP obligations, even if those functions will proceed automatically in the future, especially but not exclusively if the provider will continue to collect fees or realize profits, regardless of whether the profits are direct gains or indirect. The use of an automated process such as a smart contract to carry out VASP functions does not relieve the controlling party of responsibility for VASP obligations. For purposes of determining VASP status, launching a self-propelling infrastructure to offer VASP services is the same as offering them, and similarly commissioning others to build the elements of an infrastructure, is the same as building them.

~~Notably, the scope of the FATF definition includes both virtual-to-virtual and virtual-to-fiat transactions or financial activities or operations.~~

~~Depending on their particular financial activities, VASPs include VA exchanges and transfer services; some VA wallet providers, such as those that host wallets or maintain custody or control over another natural or legal person's VAs, wallet(s), and/or private key(s); providers of financial services relating to the issuance, offer, or sale of a VA (such as in an ICO); and other possible business models.~~

~~When determining whether a specific activity or entity falls within the scope of the definition and is therefore subject to regulation, countries should consider the wide range of various VA services or business models that exist in the VA ecosystem and, in particular, consider their functionality or the financial activities that they facilitate in the context of the covered VA activities (*i.e.*, items (i) through (v) described in the VASP definition above). Further, countries should consider whether the activities involve a natural or legal person that conducts as a business the five functional activities described for or on behalf of another natural or legal person, both of which are essential elements to the definition and the latter of which implies a certain level of "custody" or "control" of the virtual asset, or "ability to actively facilitate the financial activity" on the part of the natural or legal person that conducts the business for a customer.~~

~~For example, exchange between virtual assets and fiat currencies (item (i)), exchange between one or more forms of virtual assets (item (ii)), and transfer of virtual assets (item (iii)), including from one hosted wallet to another wallet owned by the same person, potentially apply to various VA exchange and transfer activities. Exchanges or exchangers can exist in various forms and business models and generally provide third-party services that enable their customers to buy and sell VAs~~

in exchange for traditional fiat currency, another VA, or other assets or commodities.[20] Exchange and/or transfer business models can include "traditional" VA exchanges or VA transfer services that actively facilitate the exchange of VA for real currency or other forms of VA and/or for precious metals for remuneration(*e.g.* for a fee, commission, spread, or other benefit). These models typically accept a wide range of payment methods, including cash, wires, credit cards, and VAs. Traditional VA exchange or transfer services can be administrator-affiliated, non-affiliated, or a third-party provider. Providers of kiosks – often called "ATMs," bitcoin teller machines," "bitcoin ATMs," or "vending machines" – may also fall into the above definitions because they provide or actively facilitate covered VA activities via physical electronic terminals (the kiosks) that enable the owner/operator to actively facilitate the exchange of VAs for fiat currency or other VAs.

Other VA services or business models may also constitute exchange or transfer activities based on items (i), (ii), and (iii) of the definition, and the natural or legal persons behind such services or models would therefore be VASPs if they conduct or facilitate the activity as a business on behalf of another person. These can include: VA escrow services, including services involving smart contract technology, that VA buyers use to send or transfer fiat currency in exchange for VAs, when the entity providing the service has custody over the funds; brokerage services that facilitate the issuance and trading of VAs on behalf of a natural or legal person's customers; order book exchange services, which bring together orders for buyers and sellers,[21] typically by enabling users to find counterparties, discover prices, and trade, potentially through the use of a matching engine that matches the buy and sell orders from users;[22] and advanced trading services that allow users to buy portfolios of VAs and access more sophisticated trading techniques, such as trading on margin or algorithm-based trading.

Peer-to-peer trading platforms are websites that enable buyers and sellers of VAs to find one another. Some trading platforms also facilitate trades as an intermediary. Depending on a jurisdiction's national legal framework, if a VA trading platform only provides a forum where buyers and sellers of VAs can post their bids and offers (with or without automatic interaction of orders), and the parties themselves trade at an outside venue (either through individual wallets or other wallets not hosted by the trading platform – *i.e.*, an individual user-to-individual user transaction), then the platform may not constitute a VASP as defined above. However, where the platform facilitates the exchange, transfer, or other financial activity involving VAs (as described in items (i) through (v), including by purchasing VAs from a seller when transactions or bids and

---

[20] In many jurisdictions, the term "exchange" is broad and can refer to both money transmission exchanges as well as to any organization, association, or group of persons, whether incorporated or unincorporated, that constitutes, maintains, or provides a market place or facilities for bringing together purchases and sellers or for otherwise performing (*e.g.*, with respect to securities) the functions commonly performed by a stock exchange as that term is generally understood and includes the market place and the market facilities maintained by the exchange.

[21] Countries should assess the totality of activities and technology used to bring together orders of multiple buyers and sellers for securities using established non-discretionary methods under which such orders interact. A system brings together orders of buyers and sellers if, for example, it displays or otherwise represents trading interest entered on a system to users or if the system receives users' orders centrally for future processing and execution.

[22] The example of an order-book exchange service provided here describes a typical "order book," which is usually a website interface that collects and displays orders for buyers and sellers and lets users find counterparties, discover prices, and trade through a matching engine. is an example of an online platform that allowed buyers and sellers to trade Ether and ERC20 tokens in secondary market trading involving a VA order-book exchange service that provided a user interface with an order book to match trades and send them to be recorded on the distributed ledger. (In contrast, a peer-to-peer exchange platform is more akin to a bulletin board where one buyer and one seller might locate one another and then go to a different location to effect the trade between themselves.)

offers are matched on the trading platform and selling the VAs to a buyer, then the platform is a VASP conducting exchange and/or transfer activity as a business on behalf of its customers.

Exchange or transfer services may also occur through decentralized exchanges or platforms. "Decentralized (distributed) application (DApp)," for example, is a term that refers to software programs that operate on a peer-to-peer network of computers running a blockchain platform – a type of distributed public ledger that allows the development of secondary blockchains – designed such that they are not controlled by a single person or group of persons and thus do not have an identifiable administrator. An owner/operator of a DApp may deploy it to perform a wide variety of functions, including acting as an unincorporated organization, such as a software agency, to provide virtual asset activities.[23] Generally, a DApp user must pay a fee to the DApp, which is commonly paid in VAs, for the ultimate benefit of the owner/operator in order to run the software. When DApps facilitate or conduct the exchange or transfer of value (whether in VA or traditional fiat currency), the DApp, its owner/operator(s), or both may fall under the definition of a VASP. Likewise, a person that develops a decentralized VA payment system may be a VASP when they engage as a business in facilitating or conducting the activities previously described on behalf of another natural or legal person.

In the context of item (iv) of the VASP definition, *safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets*, countries should account for services or business models that combine the function of safeguarding the value of a customer's VAs with the power to manage or transmit the VAs independently from the owner, under the assumption that such management and transmission will only be done according to the owner's/customer's instructions. Safekeeping and administration services include persons that have exclusive or independent control of the private key associated with VAs belonging to another person or exclusive and independent control of smart contracts to which they are not a party that involve VAs belonging to another person.

Natural or legal persons that actively facilitate the offer or issuance of and trading in VAs, including by accepting purchase orders and funds and purchasing VAs from an issuer to resell and distribute the funds or assets, may also fall within the scope of items (i), (ii), and (iii) as well as within item (v), participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.[24] For example, ICOs are generally a means to raise funds for new projects from early backers and the natural and legal persons actively facilitating the issuance may provide services that involve exchange or transfer activity as well as issuance offer and/or sale activity.

A jurisdiction's applicable AML/CFT obligations governing service providers that participate in or provide financial services relating to an issuer's offer and/or sale, such as in the context of ICOs, may therefore involve both the jurisdiction's money transmission regulations as well as its regulations governing securities, commodities, or derivatives activities.

A VASP may fall into one or more of the five categories of activity or operation described under the VASP definition (*i.e.*, "exchange" of virtual/fiat, "exchange" of virtual/virtual, "transfer," "safekeeping and/or administration," and "participation in and provision of financial services related to an issuer's offer and/or sale").

For example, a number of online platforms that provide a mechanism for trading assets, including VAs offered and sold in ICOs, may meet the definition of an exchange and/or a security-related entity dealing in VAs that are "securities" under various jurisdictions' national legal frameworks. Other jurisdictions may have a different approach which may include payment tokens. The relevant

[23] For an example of a DApp, *see* the U.S. Securities and Exchange Commission (SEC)'s Release No. 81207/ July 25, 2017, "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO," available at.

[24] Activity (v). aims to cover similar activities, conducted in a VA context, as the ones described in Activity 8 of the FATF definition of Financial institutions "*Participation in securities issues and the provision of financial services related to such issues" (FATF Glossary)*

competent authorities in jurisdictions should therefore strive to apply a functional approach that takes into account the relevant facts and circumstances of the platform, assets, and activity involved, among other factors, in determining whether the entity meets the definition of an "exchange" or other obliged entity (such as a securities-related entity) under their national legal framework and whether an entity falls within a particular definition. In reaching a determination, countries and competent authorities should consider the activities and functions that the entity in question performs, regardless of the technology associated with the activity or used by the entity.

Whether a natural or legal person engaged in VA activities is a VASP depends on how the person uses the VA and for whose benefit. As emphasized above, if a person (natural or legal) is engaged as a business in any of the activities described in the FATF definition (*i.e.*, items (i) through (v)) for or on behalf of another person, then they are a VASP, regardless of what technology they use to conduct the covered VA activities. Moreover, they are a VASP, whether they use a decentralized or centralized platform, smart contract, or some other mechanism. However, a person not engaging as a business for or on behalf of another natural or legal person in the aforementioned activities (*e.g.*, an individual who obtains VAs and uses them to purchase goods or services on their own behalf or makes a one-off exchange or transfer) is not a VASP.

Just as the FATF does not seek to regulate the individual users (not acting as a business) of VAs as VASPs – though recognizing that such users may still be subject to compliance obligations under a jurisdiction's sanctions or enforcement framework[25] – the FATF similarly does not seek to capture the types of closed-loop items that are non-transferable, non-exchangeable, and non-fungible. Such items might include airline miles, credit card awards, or similar loyalty program rewards or points, which an individual cannot sell onward in a secondary market. Rather, the VA and VASP definitions are intended to capture specific financial activities and functions (*i.e.*, transfer, exchange, safekeeping and administration, issuance, etc.) and assets that are fungible – whether virtual-to-virtual or virtual-to-fiat.

Likewise, the FATF does not seek to regulate the technology that underlies VAs or VASP activities, but rather the natural or legal persons behind such technology or software applications that may use technology or software applications to facilitate financial activity or conduct as a business the aforementioned VA activities on behalf of another natural or legal person. A person that develops or sells either a software application of a new VA platform (*i.e.*, a software developer) may therefore not constitute a VASP when solely developing or selling the application or platform, but they may be a VASP if they also use the new application or platform to engage as a business in exchanging or transferring funds or conducting any of the other financial activity described above on behalf of another natural or legal person. Further, the FATF does not seek to regulate as VASPs natural or legal persons that provide ancillary services or products to a virtual asset network, including hardware wallet manufacturers and non-custodial wallets, to the extent that they do not also engage in or facilitate as a business any of the aforementioned covered VA activities on behalf of their customers.

Importantly, in INR. 15, the FATF does not exempt specific assets based on terms that may lack a common understanding across jurisdictions or even among industry (*e.g.*, "utility tokens"), in part so that Recommendation 15 and its Interpretive Note may continue to be technology neutral. Rather, the framing of the Recommendations, including Recommendation 15, is activity-based and focused on functions in order to provide jurisdictions with sufficient flexibility.

Flexibility is particularly relevant in the context of VAs and VA activities, which involve a range of products and services in a rapidly-evolving space. Some items – or tokens – that on their face do not appear to constitute VAs may in fact be VAs that enable the transfer or exchange of value or facilitate ML/TF.

[25] In the United States, for example, such "users" must, like all U.S. persons or persons otherwise subject to U.S. jurisdiction, comply with all U.S. sanctions and regulations administered by the U.S. Department of the Treasury's Office of Foreign Assets Control. Further, U.S. sanctions compliance obligations are the same, regardless of whether a transaction is denominated in digital currency or traditional fiat currency or involves some other form of asset or property.

~~Some ICOs, for example, relate to or involve "gaming tokens," and other "gaming tokens" can be used to obfuscate transaction flows between an in-game token and its exchange for or transfer to a VA. Secondary markets also exist in both the securities and commodities sectors for "goods and services" that are fungible and transferable. For example, users can develop and purchase certain virtual items that act as a store of value and in fact accrue value or worth and that can be sold for value in the VA space.~~

~~As discussed above, countries should focus on the financial conduct or activity surrounding the VA or its underlying technology and how it poses ML/TF risks (*e.g.*, the potential for enhanced anonymity, obfuscation, disintermediation, and decreased transparency or technology, platforms, or VAs that undermine a VASP's ability to perform AML or CDD) and apply measures accordingly.~~

~~Countries should address the ML/TF risks associated with VA activities, both where those activities intersect with the regulated fiat currency financial system, as appropriate under their national legal frameworks, which may offer various options for regulating such activity, as well as where such activities may not involve the fiat currency financial system but consist only of "virtual-to-virtual" interactions (*e.g.*, as in the case of exchanges between one or more forms of VA).~~

~~Similarly, AML/CFT regulations will apply to covered VA activities and VASPs, regardless of the type of VA involved in the financial activity (*e.g.*, a VASP that uses or offers AECs to its customers for various financial transactions), the underlying technology, or the additional services that the platform potentially incorporates (such as a mixer or tumbler or other potential features for obfuscation).~~

Section III – Application of FATF Standards to Countries and Competent Authorities

45.80. Section III explains how the FATF Recommendations relating to VAs and VASPs apply to countries and competent authorities and focuses on identifying and mitigating the risks associated with covered VA activities, applying preventive measures, applying licensing and registration requirements, implementing effective supervision on par with the supervision of related financial activities of FIs, providing a range of effective and dissuasive sanctions, and facilitating national and international co-operation. Almost all of the FATF Recommendations are directly relevant for understanding how countries should use government authorities and international co-operation to address the ML/TF risks associated with VAs and VASPs, while other Recommendations are less directly or explicitly linked to VAs or VASPs, though they are still relevant and applicable.

46.81. VAs and VASPs are subject to the full range of obligations under the FATF Recommendations, as described in INR. 15, including those obligations applicable to other entities subject to AML/CFT regulation, based on the financial activities in which VASPs engage and having regard to the ML/TF risks associated with covered VA activities or operations.

47.82. This section also reviews the application of the risk-based approach by supervisors of VASPs.

Application of the Recommendations in the Context of VAs and VASPs

Risk-Based Approach and National Co-ordination

48.83. **Recommendation 1.** The FATF Recommendations make clear that countries should apply a risk-based approach to ensure that measures to prevent or mitigate ML/TF risks are commensurate with the risks identified in their respective jurisdictions. Under the risk-based approach, countries should strengthen the requirements for higher-risk situations or activities involving VAs. When assessing the ML/TF risks associated with VAs, the particular types of VA financial activities, such as P2P transactions for instance, and the activities or operations of VASPs, the distinction between centralized and decentralized VAs and whether they are subject to control by a regulated VASP, as discussed in the 2015 VC Guidance, will likely continue to be a key aspect for countries to consider. Due to the potential for increased anonymity or obfuscation of VA financial flows and the challenges associated with conducting effective supervision and ~~customer~~ CDD, including customer identification and verification, VAs and VASPs in general may be regarded as higher ML/TF risks that may potentially require the application of monitoring and enhanced due diligence measures, where appropriate, depending on the jurisdiction's context.

84. Recommendation 1 requires countries to identify, understand, and assess their ML/TF risks and to take action aimed at effectively mitigating those risks. The requirement applies in relation to the risks associated with new technologies under Recommendation 15, including VAs and the risks associated with VASPs that engage in or provide covered VA activities, operations, products, or services. Public-private sector co-operation may assist competent authorities in developing AML/CFT policies for covered VA activities (*e.g.*, VA payments, VA transfers, VA issuance, etc.) as well as for innovations in related VA technologies and emerging products and services, where appropriate and applicable. Co-operation may also assist countries in allocating and prioritizing AML/CFT resources by competent authorities.

85. The FATF amended Recommendation 1 and its Interpretive Note in October 2020 to include a requirement for countries, financial institutions and DNFBPs to assess

proliferation financing (PF) risks as defined under the Standards. Further, separate guidance is under development by the FATF to clarify these requirements. That guidance is relevant for the assessment and mitigation of PF risks by countries and VASPs. Countries should identify, assess and take effective action to mitigate the ML/TF/PF risks related to VAs.

~~3.~~

~~49.~~86. National authorities should undertake a co-ordinated risk assessment of VA activities, products, and services, as well as of the risks associated with VASPs and the overall VASP sector in their country, if any. The risk assessment should (i) enable all relevant authorities to understand how specific VA products and services function, fit into, and affect all relevant regulatory jurisdictions for AML/CFT purposes (*e.g.*, money transmission and payment mechanisms, VA kiosks, VA commodities, VA securities or related issuance activities, etc., as highlighted in the VASP definition) and (ii) promote similar AML/CFT treatment for similar products and services with similar risk profiles.

~~50.~~87. 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 and investor 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.

88. Countries should also require VASPs (as well as other obliged entities) to identify, assess, and take effective action to mitigate the ML/TF risks associated with providing or engaging in covered VA activities or associated with offering particular VA products or services. Where VASPs are permitted under national law, countries, VASPs, as well as FIs and DNFBPs—including FIs or DNFBPs that engage in VA activities or provide VA products or services—must assess the associated ML/TF risks and apply a risk-based approach to ensure that appropriate measures to prevent or mitigate those risks are implemented.

So-called stablecoins

89. It is important that ML/TF risks of so-called stablecoins, particularly those with potential for mass-adoption and can be used for P2P transactions, are analysed in an ongoing and forward-looking manner and are mitigated before such arrangements are launched. It will be more difficult to mitigate risks of these products once they are launched.

90. Where there is a central developer and governance body which is a FI or a VASP at any stage of development, it is critical that national AML/CFT supervisors ensure that the body is taking adequate steps to mitigate the ML/TF risks, before launch where the preparatory activities mean that the entity is a FI or a VASP, and on an ongoing basis. Such a body can be held accountable for the implementation of AML/CFT controls across the arrangement and for taking steps to mitigate ML/TF risks (e.g. in the design of the so-called stablecoin). This could include, for example, limiting the scope of customers' ability to transact anonymously and/or by ensuring that AML/CFT obligations of obliged entities within the arrangement are fulfilled, e.g. by using software to monitor transactions and detect suspicious activity. Not all so-called stablecoins may have a readily identified central body which is a VASP or a FI one launched. However, it may be more likely that a party needs to exist to drive the development and launch of such an arrangement before its release. If this entity was a business and carried out VASP functions, this would create scope for regulatory or supervisory action in the pre-launch phase.

P2P transactions

91. Countries should also seek to understand the ML/TF risks related to P2P transactions and how P2P transactions are being used in their jurisdiction. Countries may consider the following non-exhaustive list of options to mitigate risks posed by P2P transactions at a national level if the ML/TF risks are unacceptably high. This includes measures that seek to bring greater visibility to P2P transactions, as well as to limit jurisdiction's exposure to P2P transactions. These measures may include:

    a) controls that facilitate visibility of P2P activity and VA activity crossing between obliged entities and non-obliged entities (these controls could include VA equivalents to currency transaction reports or reporting of cross-border instrument transfers);

    b) ongoing enhanced supervision of VASPs and entities operating in the VA space with a feature enabling unhosted wallet transactions (*e.g.*, on-site and off-site supervision to confirm whether a VASP has compiled with the regulations in place concerning these transactions);

    c) denying licensing of VASPs if they allow transactions to/from non-obliged entities (*i.e.,* private / unhosted wallets) (*e.g.,* oblige VASPs via the 'travel rule' to accept transactions only from/to other VASPs);

    d) placing additional AML/CFT requirements on VASPs that allow transactions to/from non-obliged entities (e.g. enhanced recordkeeping requirements, enhanced due diligence (EDD) requirements); and

    e) guidance highlighting the importance of VASPs applying risk-based approach to dealing with customers that engage in, or facilitate, P2P transactions, supported by risk assessment, indicators or typologies publications where appropriate.

92. Additional measures that countries may wish to consider assist in understanding and mitigating the risks of P2P transactions include:

    a) outreach to the private sector, including VASPs and representatives from the P2P sector (e.g. consulting on AML/CFT requirements concerning P2P transactions);

    b) issuing public guidance and advisories and conducting information campaigns to raise awareness of risks posed by P2P transactions; and

    c) training of supervisory, FIU and law enforcement personnel.

93. In addition to P2P transactions between unhosted wallets, the FATF has identified other potential risks which may require further action, including; VAs located in jurisdictions with weak or non-existent AML/CFT frameworks (which would not properly implement AML/CFT preventive measures) and VAs with decentralised governance structures (which may not include an intermediary that could apply AML/CFT measures).[26] These risks may require jurisdictions or VASPs to identify VASP- or country-specific risks and implement specific safeguards for transactions that have a nexus to VASPs and jurisdictions lacking in regulation, supervision, or appropriate controls. These risks are particularly heightened for so-called stablecoins with potential for mass-adoption.

Prohibition or limitation of VAs/VASPs

94. A jurisdiction has the discretion to prohibit or limit VA activities or VASPs, and those VA activities carried out by non-obliged entities, based on their assessment of risk and national

[26] See the FATF's report to G20 on so-called stablecoins for further information.

regulatory context or in order to support other policy goals not addressed in this Guidance (*e.g.*, consumer and investor protection, safety and soundness, or monetary policy). This can include a ban or limitation on the activity in general, or specific bans or limitations on products or services which are deemed to pose an unacceptable level of risk.

95. Where countries consider prohibiting VA activities or VASPs, they should take into account the effect that such a prohibition may have on their ML/TF risks. Regardless of whether a country opts to prohibit or regulate activities in the sector, additional measures may be useful in mitigating the overall ML/TF risks. For example, if a country prohibits VA activities and VASPs, mitigation measures should include identifying VASPs (or other obliged entities that may engage in VA activities) that operate illegally in the jurisdiction and applying proportionate and dissuasive sanctions to such entities, and the risk that services will be offered in that country by a VASP based abroad. Based on the country's risk profile, prohibition should still require outreach and enforcement actions by the country as well as risk mitigation strategies that account for the cross-border element of VA activities (*e.g.*, cross-border VA payments or transfers) and VASP operations.

~~51.~~96. Recommendation 2 requires national co-operation and co-ordination with respect to AML/CFT/~~–~~CPF policies, including in the VASP sector, and is therefore indirectly applicable to countries in the context of regulating and supervising covered VA activities. Countries should consider putting in place mechanisms, such as interagency working groups or task forces, to enable policymakers, regulators, supervisors, the financial intelligence unit (FIU), and law enforcement authorities to co-operate with one another and any other relevant competent authorities in order to develop and implement effective policies, regulations, and other measures to address the ML/TF/PF risks associated with covered VA activities and VASPs. This should include co-operation and co-ordination between relevant authorities to ensure the compatibility of AML/CFT requirements with Data Protection and Privacy rules and other similar provisions (e.g., data security/localisation). National co-operation and co-ordination are particularly important in the context of VAs, in part due to their highly-mobile and cross-border nature and because of the manner in which covered or regulated VA activities may implicate multiple regulatory bodies (e.g., those competent authorities regulating money transmission, securities, and commodities or derivatives activities). Further, national co-operation relating to VA issues is vital in the context of furthering investigations and leveraging various interagency tools relevant for addressing the cyber and/or VA ecosystem.

Treatment of Virtual Assets: Interpreting the Funds- or Value-Based Terms

~~52.~~97. For the purposes of applying the FATF Recommendations, countries should consider all funds- or value-based terms in the Recommendations, such as "property," "proceeds," "funds," "funds or other assets," and other "corresponding value," as including VAs. In particular, countries should apply the relevant measures under Recommendations 3 through 8, 30, 33, 35, and 38, all of which contain references to the aforementioned funds- or value-based terms or other similar terms, in the context of VAs in order to prevent the misuse of VAs in ML, TF, and ~~proliferation financing~~ (PF~~)~~ and take action against all proceeds of crime involving VAs. The aforementioned Recommendations—some of which may not at first appear directly applicable to VASPs and similarly obliged entities but are in fact applicable in this space—relate to the ML offence, confiscation and provisional measures, TF offence, targeted financial sanctions, non-profit organisations, law enforcement powers, sanctions, and international co-operation.

~~53.~~98. **Recommendation 3.** For the purposes of implementing Recommendation 3, the ML offence should extend to any type of property, regardless of its value, that directly represents the proceeds of crime, including in the context of VAs. When proving that

property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence, including in the case of VA-related proceeds. Countries should therefore extend their applicable ML offence measures to proceeds of crime involving VAs.

~~54.~~99. **Recommendation 4.** Similarly, the confiscation and provisional measures relating to "(a) property laundered, (b) proceeds from, or instrumentalities used in or intended for use in money laundering or predicate offences, (c) property that is used in, or intended or allocated for use in, the financing of terrorism, terrorist acts, or terrorist organisations, (d) or property of corresponding value" also apply to VAs.

~~55.~~100. As for confiscation or temporary measures applicable to fiat currencies and goods, ~~law enforcement authorities (~~LEAs~~)~~ should be able to request a temporary freeze of assets when there are grounds to establish or when it is established, that they originate from criminal activity. To extend the duration of the freeze or to request the confiscation of assets, LEAs should obtain a court order.

~~56.~~101. **Recommendation 5.** Likewise, the TF offences described in Recommendation 5 should extend to "any funds or other assets," including VAs, whether from a legitimate or illegitimate source (see INR. 5).

~~57.~~102. **Recommendation 6.** Countries should also freeze without delay the funds or other assets—including VAs—of designated persons or entities and ensure that no funds or other assets—including VAs—are made available to or for the benefit of designated persons or entities in relation to the targeted financial sanctions related to terrorism and terrorist financing.

~~58.~~103. **Recommendation 7.** In the context of targeted financial sanctions related to proliferation, countries should freeze without delay the funds or other assets—including VAs—of designated persons or entities and ensure that no funds or others assets—including VAs—are made available to or for the benefit of designated persons or entities.

~~59.~~104. **Recommendation 8.** Countries also should apply measures, in line with the risk-based approach, to protect non-profit organisations from ~~terrorist financing~~TF abuse, as laid out in Recommendation 8, including when the clandestine diversion of funds to terrorist organisations involves VAs (see Recommendation 8(c)).

~~60.~~105. **Recommendation 30** applies to covered VA activities and VASPs in the context of the applicability of all funds- or value-based terms addressed in sub-section 3.1.2 of this Guidance. As with other types of property or proceeds of crime, countries should ensure that competent authorities have responsibility for expeditiously identifying, tracing, and initiating actions to freeze and seize VA- related property that is, or may become, subject to confiscation or is suspected of being the proceeds of crime. Countries should implement Recommendation 30, regardless of how the jurisdiction classifies VAs in its national legal framework (*i.e.*, regardless of how VAs are categorized legally with respect to the property laws of the jurisdiction).

~~61.~~106. **Recommendation 33.** The statistics that countries maintain should include statistics on the ~~suspicious transaction reports (~~STRs~~)~~ that the competent authorities receive and disseminate as well as on the property that the competent authorities freeze, seize, and confiscate. Countries should therefore also implement Recommendation 33 in the context of VASPs and VA activities and maintain statistics on the STRs that competent authorities receive from VASPs and from other obliged entities, such as banks, that submit STRs relating to VASPs, VAs, or VA activities. As with other Recommendations that contain funds- or value-based terms (*e.g.,* Recommendation 3 through 8, 30, 35, and 38), countries should also maintain statistics on any VAs that competent authorities freeze, seize, or confiscate, regardless of how the jurisdiction categorizes VAs with respect to the property

laws of its national legal framework. Additionally, countries should consider updating their STRs and associated statistics to incorporate VA-related indicators that facilitate investigations and financial analysis.

~~62.~~107. **Recommendation 35** directs countries to have a range of effective, proportionate and dissuasive sanctions (criminal, civil or administrative) available to deal with natural or legal persons covered by Recommendations 6 and 8 to 23 that fail to comply with the applicable AML/CFT requirements. As required by paragraph 6 of INR. 15, countries should similarly have in place sanctions to deal with VASPs (and other obliged entities that engage in VA activities) that fail to comply with their AML/CFT requirements. As with FIs and DNFBPs and other natural or legal persons, such sanctions should be applicable not only to VASPs but also to their directors and senior management, where applicable.

~~63.~~108. **Recommendation 38** also contains funds- or value-based terms and applies in the context of VAs but is addressed in further detail in sub-section 3.1.8 on *International Co-operation* and the implementation of Recommendations 37 through 40, as described in paragraph 8 of INR. 15.

Licensing or Registration

109. Countries should designate one or more authorities that have responsibility for licensing and/or registering VASPs.

110. The FATF standards allow jurisdictions flexibility in applying licensing or registration to VASPs. Many countries are confronting the decision of whether to fit VASPs into an existing regime for licensing or registration or create a new one. Using an existing regime is likely to offer countries a quicker path to implementation and will take advantage of existing knowledge in the compliance community of how to operate the relevant processes. However, a new regime could be purpose-built for VASPs and not include legacy aspects that may not apply to VASPs. For instance, such a regime could include greater focus on technological capacity in AML/CFT analysis. While this decision ultimately rests with jurisdictions, they may find it is easier to use an existing licensing/registration system, such as that for MVTS, to the extent that their existing regimes are functional and appropriate for VASPs. It is necessary to confirm in advance that the existing system can sufficiently address the risk of VASPs. Where countries have created new laws and regulations explicitly for VAs and VASPs, a new licensing/registration system may make more sense. Jurisdictions should base the nature and stringency of the requirements and the type of regime they choose on an assessment of the different kinds of VASP activity.

Which VASPs should be licensed or registered?

~~64.~~111. In accordance with INR. 15 paragraph 3, at a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are *created*. References to creating a legal person[27] include the incorporation of companies or any other mechanism that is used domestically to formalise the existence of a legal entity, such as registration in the public register, commercial register, or any equivalent register of companies or legal entities; recognition by a notary or any other public officer; filing of the company bylaws or articles of incorporation; allocation of a company tax number, etc.

112. In cases where the VASP is a natural person, it should be required to be licensed or registered in the jurisdiction where its place of business is located—the determination of which may include several factors for consideration by countries. The place of business of

[27] See footnote 40 in INR. 24.

a natural person can be characterised by the primary location where the business is performed or where the business' books and records are kept as well as where the natural person resides (*i.e.*, where the natural person is physically present, located, or resident). When a natural person conducts business from his/her residence, or a place of business cannot be identified, his/her primary residence may be regarded as his/her place of business, for example. The place of business may also include, as one~~a~~ potential factor for consideration, the location of the server of the business.

~~–~~Jurisdictions may also require VASPs that offer products and/or services to customers in, or that conduct operations from, their jurisdiction to be licensed or registered in the jurisdiction. Host jurisdictions may therefore require registration or licencing of VASPs whose services can be accessed by or are made available to people residing or living within their jurisdiction, or may require VASPs that have employees or management located in their jurisdiction. While coverage of these entities is not required by the FATF S~~s~~tandards, jurisdictions may find it to be useful in mitigating risks, particularly in view of the inherent cross-border availability of VAs. When in doubt, jurisdictions may consider that broader coverage is the safer course, as VAs will introduce whatever risks they carry with them in any jurisdiction in which they are accessible, regardless of the location in which ~~their legal entity was created~~they are incorporated.

113. In order to identify those VASPs offering products and/or services to customers in a jurisdiction without being incorporated in this jurisdiction, supervisors may use a set of relevant criteria. This could include the location of offices and servers (including customer-facing operations such as call centers), promotional communications targeting specific countries/markets, the language on the VASP website and/or mobile application, whether the VASP has a distribution network in a country (*e.g.*, if it has appointed an intermediary to seek clients or physically visit clients resident in the country), and specific information asked to customers revealing the targeted country.

How to identify VASPs for licensing or registration

114. Countries should take action to identify natural or legal persons that carry out VA activities or operations without the requisite license or registration and apply appropriate sanctions, including in the context of traditional ~~covered~~obliged entities that may engage in VA activities or operations (*e.g.*, a bank that provides VAs to its customers). National authorities should have mechanisms to monitor the VASP sector as well as other ~~covered~~obliged entities that may engage in covered VA activities or operations or provide covered VA products or services and ensure that appropriate channels are in place for informing VASPs and other ~~covered~~obliged entities of their obligation to register or apply for a license with the relevant authority. Countries should also designate an authority responsible for identifying and sanctioning unlicensed or unregistered VASPs (as well as other obliged entities that engage in VA activities). As discussed above in the Guidance, even countries that choose to prohibit VA activities or VASPs in their jurisdiction should have in place tools and authorities to identify and take action against natural or legal persons that fail to comply with their legal obligations, as required under Recommendation 15.

115. 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:

a) blockchain or distributed ledger analytics tools, as well as other investigative tools or capabilities;

b) web-scraping and open-source information to identify online advertising or possible solicitations for business by an unregistered or unlicensed entity;

c) information from the general public and industry circles (including by establishing channels for receiving public feedback) regarding the presence of certain businesses that may be unlicensed or unregistered;

d) 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;

e) non-publically available information, such as whether the entity previously applied for a license or registration or had its license or registration withdrawn; and

f) law enforcement and intelligence reports ~~blockchain or distributed ledger analytics tools, as well as other investigative tools or capabilities~~.

Considerations for licensing or registering VASPs

~~4.~~

116. VASPs that are licensed or registered should be required to meet appropriate licensing and registration criteria set by relevant authorities. These criteria should give national supervisors confidence that the concerned VASPs will be able to comply with their AML/CTF obligations. To that end, the criteria should include, as for most FIs, the obligation to demonstrate that, prior to launch, their AML/CFT programs, including policies, procedures and organization taking into account the characteristics of the VASP's activity (*i.e.,* types of VAs and transactions, targeted customers, distribution channels), are implemented or able to be implemented once launched. The assessment of these criteria is all the more efficient when it is performed in the course of the licensing or the registration process and when there is time to ensure risk controls are in place prior to launch.

117. When a jurisdiction establishes its licencing or registration scheme for VASPs, a significant number of VASPs may seek licencing or registration at the same time. To enable a smooth process, relevant authorities may consider how to ensure that sufficient flexibility is built into their approach, to allow for prioritisation of incoming requests. This could involve identifying and prioritising entities carrying out the highest risk activities for early registration, monitoring key risk indicators, or increased emphasis on ad-hoc onsite and off-site reviews by supervisors, and engaging regularly with industry bodies. If, conversely, activities are suspended pending registration, jurisdictions may wish to consider beginning with the easiest applications first and then moving on to the higher risk or more complex applicants thereafter. Countries may consider a range of other factors but should prioritize based on their judgement and capacity.

~~65. Authorities should impose such conditions on licensed or registered VASPs to be able to effectively supervise the VASPs. Such conditions should allow for sufficient supervisory hold and could potentially include, depending on the size and nature of the VASP activities, requiring a resident executive director, substantive management presence, or specific financial requirements.~~

~~66.~~1. ~~Jurisdictions may also require VASPs that offer products and/or services to customers in, or that conduct operations from, their jurisdiction to be licensed or registered in the jurisdiction. Host jurisdictions may therefore require registration or licencing of VASPs whose services can be accessed by or are made available to people residing or living within their jurisdiction, or may require VASPs that have employees or management located in their jurisdiction. While coverage of these entities is not required by the standards, jurisdictions may find it to be useful in mitigating risks, particularly in view of~~

~~the inherent cross-border availability of VAs. When in doubt, jurisdictions may consider that broader coverage is the safer course, as VAs will introduce whatever risks they carry with them in any jurisdiction in which they are accessible, regardless of the location in which their legal entity was created.~~

118. In the licensing or registration process, ~~C~~competent authorities should take the necessary legal or regulatory measures to prevent criminals, non-fit and proper persons or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a VASP. Such measures should include requiring VASPs to seek authorities' prior approval for substantive changes in shareholders, business operations, and structures.

119. On the basis of risk, authorities may also impose conditions on VASPs seeking a license or registration to be able to effectively supervise the VASPs. Such conditions could potentially include, depending on the size and nature of the VASP activities, requiring a resident executive director, substantive management presence, specific financial requirements and/or requirements for VASPs to disclose the registration(s) / license(s) which they hold in marketing materials, website and mobile applications. Authorities may also require that appropriate AML/CFT mitigations must be built into products and services before they are brought to market, as it is much more difficult to do so later. Therefore, careful assessment of risks and thorough evaluation of mitigation measures at the licensing and registration stage is especially important. Once licensing and registration has taken place, AML/CFT mitigations which are built into products and services should be maintained and be the subject of active supervision.

120. Like other entities subject to AML/CFT standards and sanctions obligations through the FATF Standards, VASPs should put in place AML/CFT compliance prior to launch when designing or building a new product or service pursuant to R. 15. Importantly, jurisdictions may consider emphasizing these requirements to VASPs through public communication and events (*i.e.,* education campaigns, forums or "office hours" with the VA ecosystem). Providing certainty concerning the legal framework through advisories or guidance is another key measure to support a culture of compliance. Countries may also consider the incentive effect of publicity of enforcement actions against unregistered or unlisensed VASPs. Furthermore, subject to their own discretion, jurisdictions may also consider designating all VASPs from countries which do not effectively implement licensing or registration requirements as high risk customers or counter-parties, so that for a VASP to deal with a counterpart in a country without an effective licensing regime is designated high risk activity by the supervisor and may incur additional reporting requirements (also see the information on EDD in Recommendation 10 in Section III and on counterparty VASP due diligence in Recommendation 16 in Sections III and IV).

~~67.~~121. All jurisdictions should encourage a culture of compliance with all of a jurisdictions' applicable legal and regulatory requirements. These may address a range of policy objectives, including those related to investor and consumer protection, market integrity, prudential requirements, and/or national and economic interests, in addition to AML/CFT. To that end, some jurisdictions may decide to underscore this by not permitting VASPs to obtain a license from prudential or other authorities which is separate from AML/CFT-related authorization. Jurisdictions should also ensure that VASPs and authorities devote sufficient resources to their AML/CFT compliance functions to cope with expected customer and transaction volume.

122. As previously noted, the distinguishing technical feature of so-called stablecoins is a stabilization mechanism. An assessment of the ML/TF risks and mitigation of the risks associated with this mechanism should form part of the licensing or registration process. Supervisors should be especially cautious of claims that so-called stablecoins involve no

entity that qualifies as a VASP. Because of the need for developers to create a stabilization mechanism, even if it is automated once launched (i.e., an algorithmic so-called stablecoin), so-called stablecoins are even more likely than some VAs to involve a VASP or FI in their creation and launch. As discussed in the FATF report to the G20, so-called stablecoins may also be more likely to reach mass adoption by the public as compared to some VAs, which could potentially greatly increase the risks they pose if realized. Therefore, the potential for mass adoption should be included as a factor meriting consideration in the licensing or registration procedure and risk assessment for all VASPs. As a general matter, however, the AML/CFT aspects of licensing or registration procedure for VASPs and obliged entities launching, or involved in, so-called stablecoins should be similar to that for VAs, except for the need to consider the stabilization mechanism.

~~Countries should take action to identify natural or legal persons that carry out VA activities or operations without the requisite license or registration and apply appropriate sanctions, including in the context of traditional covered entities that may engage in VA activities or operations (e.g., a bank that provides VAs to its customers). National authorities should have mechanisms to monitor the VASP sector as well as other covered entities that may engage in covered VA activities or operations or provide covered VA products or services and ensure that appropriate channels are in place for informing VASPs and other covered entities of their obligation to register or apply for a license with the relevant authority. Countries should also designate an authority responsible for identifying and sanctioning unlicensed or unregistered VASPs (as well as other obliged entities that engage in VA activities). As discussed above in the Guidance, even countries that choose to prohibit VA activities or VASPs in their jurisdiction should have in place tools and authorities to identify and take action against natural or legal persons that fail to comply with their legal obligations, as required under Recommendation 15.~~

~~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-publically 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; blockchain or distributed ledger analytics tools, as well as other investigative tools or capabilities.~~

Co-operation with domestic and international partners

123. Co-ordination between various national authorities involved in the regulation and licensing or registration of VASPs is important, as described previously in the context of Recommendation 2, since various authorities may hold information relating to unauthorised providers or activities. This is particularly important for situations where a country has multiple different licensing or registration schemes for VASPs, rather than one central regime.

124. International co-operation in the registration and licencing process is also important. Authorities may also inform their counterparties that VASPs, which they have previously registered or licensed, are operating in their counterparties' jurisdictions. Countries should have in place relevant channels for sharing information as appropriate to

support the identification and sanctioning of unlicensed or unregistered VASPs. Authorities should also consider the Principles of Information-Sharing and Co-operation amongst VASP Supervisors for further guidance on how to co-operate with counterparts in the licensing or registration process (see **Section VI).**

Supervision or Monitoring

125. **Recommendations 26 and 27.** As discussed below, Recommendation 15 requires countries to subject VASPs to effective systems for AML/CFT supervision or monitoring. As set forth in Recommendation 26 and 27, paragraph 5 of INR. 15 similarly requires countries to ensure that VASPs are also subject to adequate regulation and supervision or monitoring for AML/CFT and are effectively implementing the FATF Recommendations, in line with their ML/TF risks. VASPs should be subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements. VASPs should be supervised or monitored by a competent authority, not a self-regulatory body (SRB), which should conduct risk-based supervision or monitoring. Supervisors should have adequate powers to supervise or monitor and ensure compliance by VASPs (as well as other obliged entities that engage in VA activities) with requirements to combat money laundering and terrorist financing including the authority to conduct inspections, access books and records, compel the production of information, and impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict, or suspend the VASP's license or registration, where applicable. Jurisdictions should consider measures to make it sufficiently clear to foreign counterparts whom to address for the widest range of international co-operation.

~~68.~~

~~69.~~126. Given the cross-border nature of VASPs' activities and provision of services and the potential challenges in associating a particular VASP with a single jurisdiction, international co-operation between relevant supervisors is also of specific importance, as underlined in paragraph 8 of INR. 15 (see also sub-section 3.1.8). Jurisdictions could also refer to the relevant work of other international standard-setting bodies for useful guidance in this respect, such as the International Organization of Securities Commissions as well as the Basel Committee on Banking Supervision.[28]

~~70.~~127. As discussed in more detail in sub-section 3.1.9 of this Guidance, when a DNFBP engages in VASP activity, countries should subject the entity to all of the relevant measures for VASPs set forth in the FATF Recommendations, including with respect to supervision or monitoring.[29]

Preventive Measures

128. Paragraph 7 of INR. 15 makes clear that all of the preventive measures contained in Recommendations 10 through 21 apply to both countries and obliged entities in the context of VAs and VA financial activities. However, Recommendations 9, 22, and 23 also have indirect applicability in this space and are discussed below as well. Accordingly, the

[28] See, for example, Principles 3 (on co-operation and collaboration) and 13 (on home-host relationships) of the Committee's *Core Principles for Effective Banking Supervision*: www.bis.org/publ/bcbs230.pdf.

[29] As outlined in sub-section 2.2, jurisdictions may call or term VASPs as "FIs" or as "DNFBPs." However, regardless of what countries may choose to call VASPs, they are still subject to the same level of regulation and supervision as FIs, in line with the types of financial activities in which VASPs engage and the types of financial services they provide.

following sub-section provides a Recommendation-by-Recommendation explanation to help countries in further considering how to implement the preventive measures in the context of VAs. Relatedly, sub-section 4.1 provides guidance specific to VASPs and other obliged entities that engage in VA activities on how they should implement the preventive measures described below as well as other AML/CFT measures throughout the FATF Recommendations.

129. In general, the preventive measures set out in Recommendation 10 to 21 apply to VASPs in the same manner as FIs, with two specific qualifications. Firstly, the occasional transaction designated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000 (rather than USD/EUR 15 000). Secondly, the wire transfer rules set out in Recommendation 16 apply to VASPs and VA transfers in a modified form (the 'travel rule'). This is explained in more detail below.

Financial institution secrecy laws

130. **Recommendation 9** is intended to ensure that financial institution secrecy laws do not inhibit the implementation of the FATF Recommendations. As with FIs, countries should similarly ensure that secrecy laws do not inhibit the implementation of the FATF Recommendations to VASPs, although Recommendation 9 does not explicitly include or mention VASPs.

Customer due diligence

~~71.~~131. **Recommendation 10.** Countries and obliged entities should design CDD processes to meet the FATF Standards and national legal requirements. The CDD process should help VASPs (as well as other obliged entities that engage in VA activities) in assessing the ML/TF risks associated with covered VA activities or business relationships or occasional transactions above the threshold. Initial CDD comprises identifying the customer and, where applicable, the customer's beneficial owner and verifying the customer's identity on a risk basis and on the basis of reliable and independent information, data, or documentation to at least the extent required by the applicable legal or regulatory framework. The CDD process also includes understanding the purpose and intended nature of the business relationship, where relevant, and obtaining further information in higher risk situations.

~~72.~~132. In practice, VASPs typically open and maintain accounts (*i.e.*, establish a customer relationship) and collect the relevant CDD information when they provide services to or engage in covered VA activities on behalf of their customers. In cases where a VASP carries out an occasional transaction, however, the designated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000, in accordance with INR. 15, paragraph 7(a).[30]

~~73.~~133. Regardless of the nature of the relationship or transaction, countries should ensure that VASPs have in place effective procedures to identify and verify, on a risk basis, the identity of a customer, including when establishing business relations with that customer; where VASPs may have suspicions of ML/TF, regardless of any exemption of thresholds; and where they have doubts about the veracity or adequacy of previously obtained identification data.

~~74.~~134. Some jurisdictions may consider the use of VA kiosks (which some may refer to as VA "ATMs," as described in the section above on VA services and business models) as an occasional transaction, whereby the provider or owner/operator of the kiosk and the

30 The FATF agreed to lower the threshold amount for VA-related transactions to USD/EUR 1 000, given the ML/TF risks associated with and cross-border nature of VA activities.

customer using the kiosk transact on a one-off basis. Other jurisdictions may ~~require owners/operators of such kiosks (*i.e.*, the kiosk provider) to register as a VASP or other financial institution (*e.g.*, as a money transmitters) and may~~ not consider such transactions to be occasional, with resulting consequences for CDD obligations.

~~75.~~135. As discussed previously, VAs have certain characteristics that may make them more susceptible to abuse by criminals, money launderers, terrorist financiers, and other illicit actors, including their global reach, capacity for rapid settlement, ability to enable ~~"individual user-to-individual user"~~P2P transactions ~~(sometimes referred to as "peer-to-peer")~~, and potential for increased anonymity and obfuscation of transaction flows and counterparties. In light of these characteristics, countries may therefore go further than what Recommendation 10 requires by requiring ~~full~~ CDD for ~~all transactions involving VAs~~VA transfers or transactions performed by VASPs (as well as other obliged entities, such as banks that engage in VA activities), including "occasional transactions", at a threshold below the USD/EUR 1 000 threshold, in line with their national legal frameworks. Such an approach is consistent with the risk-based approach set out in Recommendation 1, provided that it is justified on the basis of the country's assessment of risks (*e.g.*, through the identification of higher risks). Additionally, jurisdictions, in establishing their regulatory and supervisory regimes, should consider how the VASP can determine and ensure that the transactions are in fact only conducted on a one-off or occasional basis rather than a more consistent (*i.e.*, non-occasional) basis. In determining what approach to take for occasional transactions, countries should take into account the product and services provided by VASPs in their jurisdiction. Countries may request VASPs to identify low risk, one-off VA transfers where the VASPs are able to accept the residual risk to inform the country's approach to occasional transactions in the VA space.

136. As described in the Interpretive Note to Recommendation 10, there are circumstances where the ML/TF risk is higher and where enhanced CDD measures must be taken. In the context of VA-related activities and VASPs, for example, countries should consider country- or geographic-specific risk factors. VASPs located in or VA transfers from or associated with particular countries present potentially higher risks for ~~money laundering or terrorist financing~~ML/TF (see INR. 10, paragraph 15(b)).

Enhanced due diligence and simplified CDD

~~76.~~137. While there is no universally agreed upon definition or methodology for determining whether a jurisdiction, in which a VASP operates or from which VA transactions may emanate, represents a higher risk for ML/TF, the consideration of country-specific risks, in conjunction with other risk factors, provides useful information for further determining potential ML/TF risks. Indicators of higher risk include:

a) Countries or geographic areas identified by credible sources[31] as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them;

b) Countries identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking, smuggling, and illegal gambling;

31 "Credible sources" refers to information that is produced by reputable and universally recognised international organisations and other bodies that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank, and the Egmont Group of Financial Intelligence Units.

c) Countries that are subject to sanctions, embargoes, or similar measures issued by international organisations such as the United Nations; and

d) Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by the FATF statements as having weak AML/CFT regimes, especially for VASPs, and for which ~~financial institutions~~VASPs and other obliged entities should give special attention to business relationships and transactions.

~~77.~~138. Countries also should consider the risk factors associated with the VA product, service, transaction, or delivery channel, including whether the activity involves pseudonymous or "anonymous transactions," "non-face-to-face business relationships or transactions," and/or "payment[s] received from unknown or un-associated third parties" (see INR. 10 15(c) as well as the examples of higher and lower risk indicators listed in paragraph 31 of this Guidance). The fact that nearly all VAs include one or more of these features or characteristics may result in countries determining that activities in this space are inherently higher risk, based on the very nature of VA products, services, transactions, or delivery mechanisms.

~~78.~~139. In these and other cases, the ~~enhanced due diligence (EDD)~~EDD measures that may mitigate the potentially higher risks associated with the aforementioned factors include:

a) corroborating the identity information received from the customer, such as a national identity number, with information in third-party databases or other reliable sources;

b) potentially tracing the customer's IP address;

~~b)~~c) the use of analysis products, such as blockchain analytics;[32] and

~~c)~~d) searching the Internet for corroborating activity information consistent with the customer's transaction profile, provided that the data collection is in line with national privacy legislation.[33]

140. Countries also should consider the ~~enhanced CDD~~ EDD measures detailed in INR. 10, paragraph 20, including obtaining additional information on the customer and intended nature of the business relationship, obtaining information on the source of funds of the customer, obtaining information on the reasons for intended or performed transactions, and conducting enhanced monitoring of the relationship and transactions. Additionally, countries should consider the measures required for FIs that engage in fiat-denominated activity that is non-face-to-face (such as mobile services) or that is comparable to VA transactions in assessing their risks and developing mitigating controls accordingly.

141. Countries may also encourage their VASPs to collect additional information on high-risk customers and transactions in case their corporate clients engage in trade finance, in order to identify, and avoid engaging in, prohibited activities, and to enable follow-up actions. Such additional information may include:

a) the purpose of transaction or payment;

b) details about the nature, end use or end user of the item;

---

[32] To date, FATF is not aware of any technically proven means of identifying the person that manages or owns an unhosted wallet, precisely and accurately in all circumstances. Countries should be aware of this and also note that the results of the analysis using such tools should be considered as reference information only.

[33] See 2015 VC Guidance, paragraph 44 as well as June 2013 Guidance for a Risk-Based Approach to New Payment Products and Services, paragraph 66.

c) proof of funds ownership;

d) parties to the transaction;

e) sources of wealth and/or funds;

f) the identity and the beneficial ownership of the counterparty; and

g) export control information, such as copies of export-control or other licenses issued by the national export control authorities, and end-user certification.

Ensuring CDD information is up-to-date

142. Additionally, countries should require VASPs and other obliged entities that engage in or provide VA products and services to keep documents, data, or information collected under the CDD process up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk customers or categories of VA products or services, and conducting ongoing due diligence (see Section IV for further discussion on ongoing due diligence and monitoring obligations for VASPs and other obliged entities). Such transactional and record reviews are vital for effective supervision and are an important data source for the transfer of the required relevant customer information for compliance with the 'travel rule' (see Recommendation 16).

Record-keeping

~~79.~~143. **Recommendation 11** requires countries to ensure that VASPs maintain all records of transactions and CDD measures for at least five years in such a way that individual transactions can be reconstructed and the relevant elements provided swiftly to competent authorities. Countries should require VASPs and other obliged entities engaging in VA activities to maintain transaction records on transactions and information obtained through CDD measures, including: information relating to the identification of the relevant parties, the public keys (or equivalent identifiers), addresses or accounts involved (or equivalent identifiers), the nature and date of the transaction, and the amount transferred, for example. The public information on the blockchain or other relevant distributed ledger of a particular VA may provide a beginning foundation for recordkeeping, provided institutions can adequately identify their customers. However, reliance solely on the blockchain or other type of distributed ledger underlying the VA for recordkeeping is not sufficient for compliance with Recommendation 11.

144. For example, the information available on the blockchain or other type of distributed ledger may enable relevant authorities to trace transactions back to a wallet address, though it may not readily link the wallet address to the name of an individual. The wallet address contains a user code that serves as a digital signature in the distributed ledger (*i.e.*, a private key) in the form of a unique string of numbers and letters. However, additional information will be necessary to associate the address to a real or natural person.

Politically exposed persons

145. **Recommendation 12** requires countries to implement measures requiring obliged entities such as VASPs to have appropriate risk management systems in place to determine whether customers or beneficial owners are foreign politically exposed persons (PEPs)[34] or

[34] "Foreign PEPs" are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, and important political party officials (FATF Glossary).

related or connected to a foreign PEP and, if so, to take additional measures beyond performing normal CDD (as defined in Recommendation 10) to determine if and when they are doing business with them, including identifying the source of funds when relevant.

Correspondent banking and other similar relationships

~~80.~~146. **Recommendation 13** stipulates that countries should require FIs to apply certain other obligations in addition to performing normal CDD measures when they engage in cross-border correspondent relationships. Separate and apart from traditional FIs that may engage in covered VA activities and for which all of the measures of Recommendation 13 already apply, some other business relationships or covered VA activities in the VASP sector may have characteristics similar to cross-border correspondent banking relationships. INR. 13 stipulates that for correspondent banking and other similar cross-border relationships, FIs should apply criteria (a) to (e) of Recommendation 13, in addition to performing normal CDD measures. "Other similar relationships" includes ~~money or value transfer services (~~MVTS~~)~~ when MVTS providers act as intermediaries for other MVTS providers or where an MVTS provider accesses banking or similar services through the account of another MVTS customer of the bank (see *2016 FATF Guidance on Correspondent Banking Relationships*).

147. As the FATF Guidance on Correspondent Banking explains[35], "correspondent banking" does not include one-off transactions or the mere messaging relationship in the context of non-customer relationships. Rather, it is characterised by its on-going, repetitive nature, with a more customer-like relationship. Correspondent banking services encompass a wide range of services which do not all carry the same level of ML/TF risks. Some correspondent banking services present a higher ML/FT risk because the correspondent institution processes or executes transactions for its customer's customers. To the extent that relationships in the VASP sector currently have or may in the future[36] have characteristics similar to cross-border correspondent banking relationships, countries should implement the preventive measures set forth in Recommendation 13 to VASPs (and other obliged entities operating in the VA space) that develop such relationships. In particular when establishing their regulatory and supervisory regimes for VASPs, countries should consider how VASPs can determine whether their counterparty VASP relationships should be categorised as a type of correspondent relationship to which Recommendation 13 applies. When the relationship involves consistent flow of transactions, and the execution of third-party payments, it may be regarded as high-risk correspondent relationship. If the relationship is not one where Recommendation 13 applies, the VASP may still need to undertake a counterparty due diligence process similar to that set out in Recommendation 13 (see Recommendation 16 for further information on counterparty VASP due diligence).

MVTS

148. **Recommendation 14** directs countries to register or license natural or legal persons that provide MVTS in the country and ensure their compliance with the relevant AML/CFT measures. As described in the 2015 VC Guidance, this includes subjecting MVTS operating in the country to monitoring for compliance with registration or licensing and other applicable AML/CFT measures. The registration and licensing requirements of

[35] Paragraph 13, Guidance on Correspondent Banking.

[36] For example, a number of researchers and analysts have indicated that they see great potential for VASPs and VA protocols to connect directly to existing correspondent banking customers and enable them to send and receive funds across borders, without the intermediation of traditional FIs, potentially leading to quicker settlements and reductions in cost.

Recommendation 15, however, apply to all VASPs, even those engaging in MVTS activities (*e.g.*, domestic entities that provide as a business convertible VA exchange services between virtual and fiat currencies in a jurisdiction).

New technologies

~~81.~~149. **Recommendation 15.** In October 2018, the FATF adopted updates to Recommendation 15, which reinforce the fundamental risk-based approach and related obligations for countries and obliged entities in the context of new technologies, in order to clarify its application in the context of VAs, covered VA financial activities, and VASPs. Recommendation 15 requires countries to identify and assess the ML/TF risks relating to the development of new products and business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Notably, it also requires countries to ensure that financial institutions licensed by or operating in their jurisdiction take appropriate measures to manage and mitigate the associated ML/TF risks before launching new products or business practices or using new or developing technologies (see Annex A).

~~82.~~150. In line with the spirit of Recommendation 15, the October 2018 update further clarifies that countries should manage and mitigate the risks emerging from VAs and ensure that VASPs are regulated for AML/CFT purposes, licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. INR. 15, which the FATF adopted in June 2019, further clarifies Recommendation 15 and defines more specifically how the FATF requirements apply in relation to VAs, covered VA activities, and VASPs, including in the context of: assessing the associated ML/TF risks; licensing or registration; supervision or monitoring; preventive measures such as CDD, recordkeeping, and suspicious transaction reporting, among others; sanctions and other enforcement measures; and international co-operation (see Annex A).

151. In the context of VA and VASP activities, countries should ensure that VASPs licensed by or operating in their jurisdiction consider whether the VASP can manage and mitigate the risks of engaging in activities that involve the use of anonymity-enhancing technologies or mechanisms, including but not limited to AECs, mixers, tumblers, and other technologies that obfuscate the identity of the sender, recipient, holder, or beneficial owner of a VA. If the VASP cannot manage and mitigate the risks posed by engaging in such activities, then the VASP should not be permitted to engage in such activities.

Wire transfers and the 'travel rule'

152. **Recommendation 16** was developed with the objective of preventing terrorists and other criminals from having unfettered access to electronically-facilitated funds transfers for moving their funds and for detecting such misuse when it occurs. At the time of drafting, the FATF termed such transfers 'wire transfers'. In accordance with the functional approach of the FATF Recommendations, the requirements relating to wire transfers and related messages under Recommendation 16 apply to all providers of such services. This includes VASPs that provide services or engage in activities, such as VA transfers, that are functionally analogous to wire transfers.

Overview of R.16 and its application to VAs and VASPs

153. Recommendation 16 defines "wire transfers" as any transaction carried out on behalf of an originator through a FI by electronic means with a view to making an amount

of funds available to a beneficiary person at a beneficiary FI, irrespective of whether the originator and the beneficiary are the same person.

154. Recommendation 16 then establishes the requirements for countries relating to wire transfers and related messages and applies to both *domestic* and *cross-border* wire transfers. In summary, countries should ensure that FIs include *required and accurate originator information*, and *required beneficiary information*, on wire transfers and related messages. FIs should also monitor wire transfers to detect those which lack the required originator and/or beneficiary information and screen the transactions to comply with relevant UNSCR resolutions (see Recommendations 6 and 7).

155. As set out in INR. 15, Countries should apply Recommendation 16 to VA transfers and VASPs. Countries should apply Recommendation 16 regardless of whether the value of the traditional wire transfer or the VA transfer is denominated in fiat currency or a VA. However, recognising the unique technological properties of VAs, Recommendation 16 applies in an amended way to VAs as set out in paragraph 7(b) of INR.15. The application of the FATF's wire transfer requirements in the VA context is called the *travel rule*.

156. The requirements of Recommendation 16 apply to VASPs whenever their transactions, whether in fiat currency or VA, involve: (a) a traditional wire transfer, or (b) a VA transfer between a VASP and another obliged entity (*e.g*, between two VASPs or between a VASP and another obliged entity, such as a bank or other FI), or (c) a VA transfer between a VASP and an unhosted wallet (i.e. a non-VASP or non-obliged entity). For transactions involving VA transfers, countries should treat all VA transfers as cross-border wire transfers, in accordance with the Interpretative Note to Recommendation 16 (INR. 16), rather than domestic wire transfers, based on the cross-border nature of VA activities and VASP operations. For transfers with unhosted wallets, the requirements of R.16 apply in a specific way, as explained below.

Requirements to obtain, hold and submit required and accurate originator and required beneficiary information

~~83.~~157. Countries should ensure that ordering institutions (whether a VASP or other obliged entity such as a FI) involved in a VA transfer, *obtain* and *hold* required and accurate originator information and required beneficiary information and *submit* the information to beneficiary institutions (whether a VASP or other obliged entity, such as a FI), if any. Further, countries should ensure that beneficiary institutions (whether a VASP or other obliged entity, such as a FI) obtain and hold required (but not necessarily accurate[37]) originator information and required and accurate beneficiary information, as set forth in INR. 16 (see Box 4 below).

Box 4. Specific wording definition

Wire transfer rules for VAs/VASPs in INR. 15-7(b)

"Recommendation 16": "Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers".

Footnote: "As defined in INR. 16, paragraph 6, or the equivalent information in a virtual asset context."

[37] As per Figure 1, data accuracy is not required for the beneficiary VASP which receives originator information from an ordering VASP. They may assume that the data has been verified by the ordering VASP.

Glossary of specific terms used in INR. 16

Accurate: is used to describe information that has been verified for accuracy.

Interpretive Note to Recommendation 16

6. Information accompanying all qualifying wire transfers should always contain:

(a) the **name of the originator**;

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

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

(d) the **name of the beneficiary**; and

(e) the beneficiary **account number** where such an account is used to process the transaction.

158. For the required information, which the *ordering* institution must *obtain* and *hold,* this includes the:

(i) originator's name (*i.e.*, the sending customer's accurate (i.e. verified) full name);

(ii) originator's account number where such an account is used to process the transaction. In the VA context, this could mean the "wallet address" of the VA and the "public key" of the customer who is sending the VA transfer;

(iii) originator's physical (geographical) address, or national identity number, or customer identification number (*i.e.*, not a transaction number) that uniquely identifies the originator to the ordering institution, or date and place of birth. For transmitting the geographical address of the customer, that means the address which has been verified for accuracy by the originator VASP as part of its KYC process (see 'Customer due diligence' above);

(iv) beneficiary's name (*i.e.*, the name of the receiving institution's customer). This is not required to be verified by the ordering institution for accuracy, but should be reviewed for the purpose of STR monitoring and sanction screening; and

(v) beneficiary account number where such an account is used to process the transaction. In the VA context, this could mean the "wallet address" of the VA and the "public key" of the person who is receiving the VA transfer as applicable.

159. For the required information which the *beneficiary* institution must *obtain* from the originator institution and *hold,* this includes the:

(i) originator's name (i.e., the sending customer's name). The beneficiary institution does not need to be verify the originator's name for accuracy, but should review it for the purpose of STR monitoring and sanction screening;

(ii) originator's account number where such an account is used to process the transaction. In the VA context, this could mean the VA's "wallet address" of the customer who is sending the VA transfer;

(iii) originator's physical (geographical) address, or national identity number, or customer identification number (i.e., not a transaction number) that uniquely identifies the originator to the ordering institution, or date and place of birth;

(iv) beneficiary's name (i.*e.*, the name of the receiving institution's customer). The beneficiary institution must verify the beneficiary's name for accuracy, if the name of their customer has not previously verified. Thus the beneficiary institution can confirm if the beneficiary's name and account number they obtain from the ordering institution match with the beneficiary institution's verified customer data; and

(v) beneficiary's account number where such an account is used to process the transaction. In the VA context, this could mean the "wallet address" of the VA and the "public key" of the person who is sending the VA transfer as applicable.

Figure 1. Data requirements for ordering and beneficiary VASPs in the travel rule

Data item and required action	Ordering VASP	Beneficiary VASP
Originator Information	✓ Required, i.e. submitting the necessary data to a beneficiary VASP is mandatory. ✓ Accurate, i.e. the ordering VASP needs to verify the accuracy as part of its CDD process.	✓ Required, i.e. the beneficiary VASP needs to obtain the necessary data from ordering VASP. ✓ Data accuracy is not required. The beneficiary VASP may assume that the data has been verified by the ordering VASP.
Beneficiary Information	✓ Required, i.e. submitting the necessary data to the beneficiary VASP is mandatory. ✓ Data accuracy is not required, but the ordering VASP must monitor to confirm no suspicions arise.	✓ Required, i.e. the beneficiary VASP needs to obtain the necessary data from the ordering VASP. ✓ Accurate, i.e. the beneficiary VASP must have verified customer data and needs to confirm if the received data is consistent.
Actions required	✓ Obtain the necessary information from its customer and retain a record. ✓ Screen to confirm that the beneficiary is not a sanctioned name ✓ Monitor transactions and report when it raises a suspicion.	✓ Obtain the necessary information from the ordering VASP and retain a record. ✓ Screen to confirm that the originator is not a sanctioned name. ✓ Monitor transaction and report when it raises a suspicion.

160. VASPs must *submit* the required information to the beneficiary institution, where this exists. It is vital that countries ensure that providers of VA transfers—whether VASPs or other obliged entities—transmit the required originator and beneficiary information *immediately* and *securely*. This is particularly relevant given the rapid and cross-border nature of VA transfers and in line with the objectives of Recommendation 16 (as well as the traditional requirement in Recommendation 16 for originator and beneficiary information to "accompany […] wire transfers" involving fiat currency). Where there is not a beneficiary institution, the VASP must still collect the required information (as set out below).

161. "*Immediately*,"— in the context of INR. 15, paragraph 7(b) and given the cross-border nature, global reach, and transaction speed of VAs—means that providers should

submit the required information simultaneously or concurrently with the transfer itself. See Section IV for additional information on these issues specific to VASPs and other obliged entities.

162. "*Securely*", also in the context of INR. 15, paragraph 7(b), is meant to convey that providers should transmit and store the required information in a secure manner. This is to protect the integrity and availability of the required information to facilitate record-keeping (among other requirements), facilitate the use of such information by receiving VASPs or other obliged entities and protect the information from unauthorized disclosure. Use of the term is not meant to impede the objectives of Recommendation 16 or Recommendation 9.

163. The submission of originator and beneficiary information in batches is acceptable, as long as submission occurs immediately and securely as per the FATF Standards. *Post facto* submission of the required information should not be permitted (*i.e.,* submission must occur before or when the VA transfer is conducted). Countries should clarify that VASPs or other obliged entities should submit the required information simultaneously with the batch VA transfer itself.

164. It is not necessary for the information to be attached directly to the VA transfer itself. The information can be submitted either directly or indirectly, as set forth in INR. 15, as long as it is submitted "*immediately and securely*" and available upon request to appropriate authorities. Consistent with the FATF's technology-neutral approach, the required information need not be communicated as part of (or incorporated into) the transfer on the blockchain or other DLT platform itself. Submitting information to the beneficiary VASP could be an entirely distinct process from that of the blockchain or other DLT VA transfer. Any technology or software solution is acceptable, provided that the solution enables the ordering and beneficiary institutions to comply with the requirements of Recommendation 16 (and does not, of course, impede their ability to comply with their other AML/CFT obligations under the FATF Recommendations). Countries should engage with their private sectors on potential applications of available technology or possible solutions for compliance with Recommendation 16 (see Section IV for additional detail specific to providers and other obliged entities in the context of Recommendation 16). It is also important to note that co-operation and co-ordination among supervisory authorities and among private sector organisations are crucial to ensure the interoperability of the travel rule solutions which VASPs adopt and to achieve the effective implementation of the travel rule globally.

165. For legal persons, the use of the Legal Entity Identifier (LEI) as **additional information** in payment messages could be possible on an optional basis.[38] To allow for the optional usage of the LEI, countries may encourage relevant stakeholders (*e.g.,* the Payment Market Practice Group in the FIs space, industry associations of VASPs, working groups in VASP sector) to work to define a common market practice for whether and how to include the LEI in the relevant VA data transfer messages alongside without changing the current message structure.

166. Countries should require both the ordering and beneficiary institution under their national frameworks to make the above required information available to appropriate

[38] CPMI - Correspondent banking – July 2016. and BCBS - Guidelines Sound management of risks related to money laundering and financing of terrorism(July 2020), "As recommended by the CPMI, the use of the LEI as additional information in payment messages should be possible on an optional basis in the current relevant payment messages (*i.e.*, MT 202 COV and MT 103). Where available, the use of the LEI would facilitate the determination by the correspondent bank that the information in the message is sufficient to unambiguously identify the originator and beneficiary of a transfer".

authorities upon request, in line with the recordkeeping requirements set forth in Recommendation 11.

167. Countries may choose to adopt a *de minimis* threshold for VA transfers of USD/EUR 1 000, having regard to the risks associated with various VAs and covered VA activities. If countries choose to implement such a threshold, there are comparatively fewer requirements for VA transfers below the threshold compared to VA transfers above the threshold. For VA transfers under the threshold, countries should require that VASPs collect:

(1) the name of the originator and the beneficiary; and

(2) the VA wallet address for each or a unique transaction reference number.

168. Such information does not need to be verified unless there are suspicious circumstances related to ML/TF, in which case information pertaining to the customer should be verified.[39]

Sanctions screening for VA transfers

169. Countries should require both ordering and beneficiary institutions to take freezing actions and prohibit transactions with designated persons and entities (*i.e.*, screening customers and required information relating to VA transfers in order to comply with their targeted financial sanctions obligations). The ordering institution should have the required information about its customer, the originator, and the beneficiary institution should have the required information about its customer, the beneficiary, in line with the CDD requirements set forth in Recommendation 10. The ordering and beneficiary institutions should have screened their customer name for compliance with targeted financial sanctions obligations at the time of onboarding their respective customer (and upon name changes). They must then screen the names of the other party (the originator or the beneficiary) when they conduct the VA transfer (see Figure 1 above).

170. Countries should require VASPs or other obliged entities to implement an effective control framework to ensure that they can comply with their targeted financial sanction obligations. This framework should take into account the nature of VA transfers. Because the required information identifying the originator and beneficiary can be held separately to the VA transfer system (*e.g.,* the blockchain), the VA transfer can be completed even with such information missing or without screening the transfer to identify suspicious and prohibited transactions. Therefore, VASPs or other obliged entities should screen required VA transfer information separately to such direct settlement. Thus, VASPs should consider remediation measures that fit their business process and the technical nature of VAs. Although blockchain technology is ever-changing, examples of controls that a VASP or other obliged entity could implement include:

a) put a customer wallet on hold until screening is completed and confirmed that no concern is raised; and

b) arrange to receive a VA transfer with a provider's wallet that links to a customer wallet. Move the transferred VA to their customer's wallet only after the screening is completed and confirmed no concern is raised.

171. Countries should be aware of this nature of VA transfers, which is different from the traditional fiat wire transfer. Thus, countries should require VASPs and other obliged entities to document their remediation control action to facilitate effective supervision.

[39] Recommendation 16, INR.16 paragraph 5.

Potentially, countries could ask obliged entities to document this control in their AML/CFT risk assessment.

VA transfers to/from other VASPs and counterparty VASP identification and due diligence

172. FATF expects countries to implement paragraph 7(b) of INR.15, taking into account the unique nature of VA transfers and the future control framework for solutions in the private sector (see Recommendation 16 in Section IV). A VA transfer can be directly settled, i.e. through distributed consensus on the blockchain between wallet addresses alone, without the need for an intermediary. For a VASP to transmit required information to another VASP however, it is necessary for them to identify their counterparty VASP and conduct due diligence on their counterparty VASP. A VASP needs to undertake counterparty VASP due diligence before they transmit the required information for compliance with paragraph 7(b) of INR.15 to their counterparty. VASPs do not need to undertake the counterparty VASP due diligence process for every VA transfer, unless there is a suspicious transaction history indicating they should. Considering the concept of due diligence, countries should expect a VASP to refresh their counterparty due diligence information periodically or when risk emerges from the relationship in line with their defined risk-based approach control structure. Accordingly, countries should expect their obliged VASPs to implement this control mechanism.

173. The best way to conduct counterparty due diligence in a timely and secure manner is a challenge.[40] There are broadly three phases in this process:

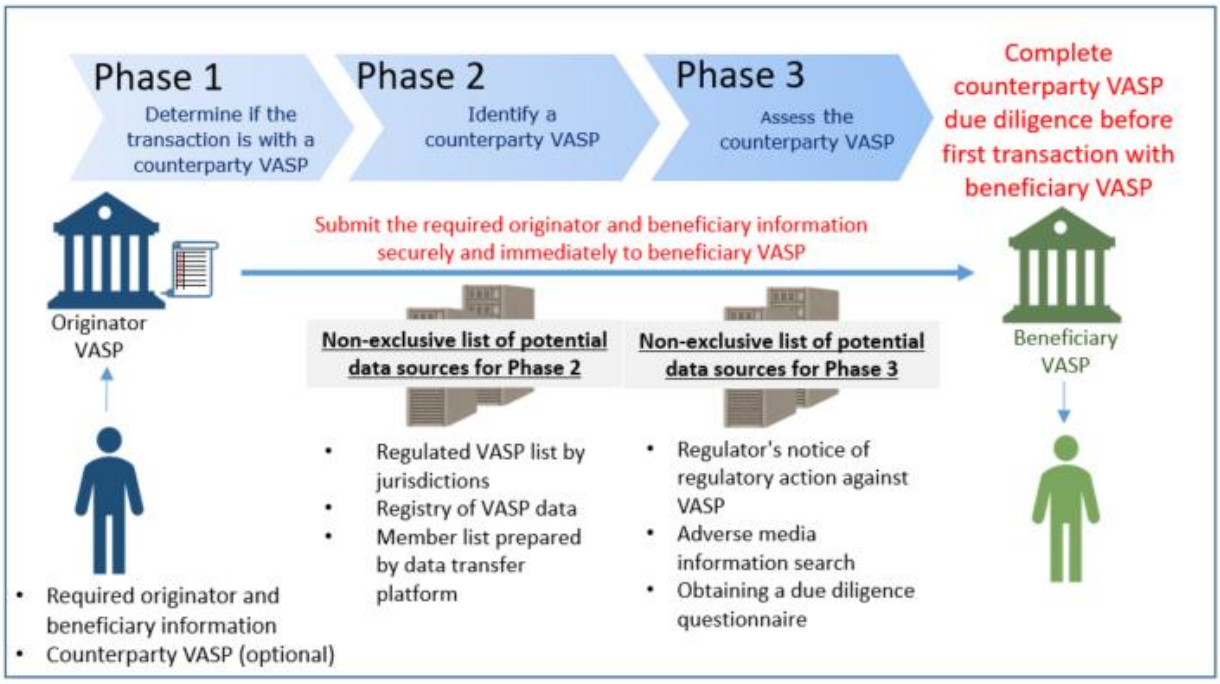
a) Phase 1: Determine whether the VA transfer is with a counterparty VASP. A customer may wish to transfer VAs to another VASP (*e.g.,* a beneficiary with a hosted wallet) or they may wish to transfer VAs to an unhosted wallet. The originator VASP must therefore determine whether they will be transacting with another VASP. This determination process is not purely an AML/CFT requirement, but rather arises from the technology underpinning VAs. To date, the FATF is not aware of any technically proven means of identifying the VASP that manages the beneficiary wallet exhaustively, precisely, and accurately in all circumstances and from the VA address alone;

b) Phase 2: Identify the counterparty VASP, as a VASP only knows the "name" of the counterparty VASP following the previous phase. A VASP may identify a counterparty VASP themselves using a reliable database in line with any guidelines from a country on when to rely on such data; and

~~a)~~c) Phase 3: Assess a counterparty VASP if they are an eligible counterparty to send customer data to and to have a business relationship with (see Recommendation 16 in Section IV for further information on counterparty VASP due diligence and Recommendation 11 on record-keeping to appropriately store and manage that customer data).

[40] See paragraph 61 of the FATF's 12-month review report.

Figure 2. Overview of counterparty VASP due diligence process



174. To clarify the scope of this Guidance, competent authorities should implement preventive measures in 'Phase 3' to assess the counterparty VASP, where VASPs first have a business relationship, and then review the results of the due diligence periodically. Countries should also maintain reliable, independent sources of information for 'Phase 2' to identify the counterparty VASP. This could include regulated institutions lists, such as VASP lists where available, registries of beneficial ownership where available and other examples mentioned in the BCBS Guideline.[41] For the benefit of effective and efficient counterparty due diligence, a regulated institutions list may especially, but not exclusively, contains the VASP name and registered VASP address. Considering the increased usage of digitalized processes in the financial industry, countries should be encouraged to use a format that is machine-readable. A country need not impose a separate licensing or registration system for VASPs with respect to natural or legal persons already licensed or registered as FIs (as defined by the FATF Recommendations) within that country. Countries that have such frameworks may clarify to their private sector that such FIs might not be on the designated VASPs lists, or even not under the supervision of the same regulator, to avoid unnecessary de-risking.

175. In addition, countries should also clarify that their VASPs should make a risk-based decision on whom to transact with, acknowledging that the risk mitigating measures taken by each individual VASP may vary. In general, those business decisions are made by each

[41] BCBS (2014, rev. 2020) Sound management of risks related to money laundering and financing of terrorism: revisions to supervisory co-operation, Annex 2" 21. Banks should also consider gathering information from public sources. These may include the website of the supervisory authority of the respondent bank, for cross-checking identification data with the information obtained by the supervisor in the licensing process, or with regard to potential AML/CFT administrative sanctions that have been imposed on the respondent bank. This may also include public registries (see FATF Guidance, paragraph 25). https://www.bis.org/bcbs/publ/d505.pdf,

individual VASP based on their risk-based analysis from an AML/CFT perspective, as well as considering other compliance issues, including data storage and security, and the profitability of the business relationship. Subject to their own discretion, jurisdictions may also consider designating all VASPs from countries which do not effectively implement licensing or registration requirements as high-risk customers or counter-parties.

176. The FATF expects jurisdictions to implement paragraph 7(b) of INR.15, taking into account the unique nature of VA transfers. Countries should take into account the unique nature of VA transfers and the developing control framework for solutions in the private sector to securely submit the required information. Nonetheless, countries are implementing their AML/CFT frameworks for VASPs at a different pace. This means that some jurisdictions will require their VASPs to comply with the travel rule prior to other jurisdictions (*i.e.,* the 'sunrise issue'). This can be a challenge for VASPs regarding what approach they should take in dealing with VASPs located in jurisdictions where the travel rule is not yet in force. Regardless of the lack of regulation in the beneficiary jurisdiction, originating entities can require travel rule compliance from beneficiaries by contract or business practice. In general, those business decisions are made by each individual VASP based on their risk-based analysis. The level of compliance that a VASP implements with paragraph 7(b) of INR. 15 should form part of those decisions. VASPs and FIs should take into account the level of ML/TF risk of each individual customer/counterparty VASP and any applicable risk mitigation measures implemented by a counterparty/customer VASP.

177. Given the 'sunrise issue' in relation to the travel rule, countries should adopt a risk-based approach in the assessment of the business models presented by VASPs. Countries should consider the full context of travel rule compliance, including whether there are sufficient risk mitigation measures taken by the VASP to adequately manage the attendant ML/TF risks. Regardless of the regulation in a certain country, a VASP may implement robust control measures to comply with the travel rule requirements. Examples include VASPs restricting VA transfers to within their customer base (*i.e.,* internal transfers of VAs within the same VASP), only allowing confirmed first-party transfers outside of their customer base (*i.e.,* the originator and the beneficiary are confirmed to be the same person) and enhanced monitoring of transactions. The absence of relevant regulations in one country does not necessarily preclude the effectiveness of measures introduced by a VASP on its own.

VA transfers to/from 'intermediary VASPs'

178. Similar to wire transfers between FIs, there may be VA transfer scenarios, either now or in the near-future, that involve "intermediary VASPs" or other intermediary obliged entities or FIs that facilitate VA transfers as an intermediate element in a chain of VA transfers. Countries should ensure that such intermediary institutions (whether a VASP or other obliged entity) also comply with the requirements of Recommendation 16, as set forth in INR. 15, including the treatment of all VA transfers as cross-border qualifying transfers. Just as a traditional intermediary FI processing a traditional fiat cross-border wire transfer must ensure that all required originator and beneficiary information that accompanies a wire transfer is retained with it, so too must an intermediary VASP or other comparable intermediary institution that facilitates VA transfers ensure that the required information is transmitted along the chain of VA transfers, as well as maintaining necessary records and making the information available to appropriate authorities upon request. Similarly, where technical limitations prevent the required originator or beneficiary information from remaining with a required data submission, a record should be kept, for at least five years, by the receiving intermediary VASP of all the information received from the ordering VASP or another intermediary VASP. Intermediary institutions involved in VA transfers

also have obligations under Recommendation 16 to identify suspicious transactions, take freezing actions, and prohibit transactions with designated persons and entities—just like ordering and beneficiary VASPs (or other ordering or beneficiary obliged entities that facilitate VA transfers).

VA transfer to/from unhosted wallets

179. The FATF recognizes that unlike traditional fiat wire transfers, not every VA transfer may involve (or be bookended by) two obliged entities, whether a VASP or other obliged entity such as a FI. In instances in which a VA transfer involves only one obliged entity on either end of the transfer *(e.g.*, when an ordering VASP or other obliged entity sends VAs on behalf of its customer, the originator, to a beneficiary that is not a customer of a beneficiary institution but rather an individual VA user who receives the VA transfer to an unhosted wallet), countries should still ensure that the obliged entity adheres to the requirements of Recommendation 16 with respect to their customer (the originator or the beneficiary, as the case may be). Countries should also consider requiring VASPs to treat such VA transfers as higher risk transactions that require enhanced scrutiny and limitations.

180. The FATF does not expect that VASPs and FIs, when originating a VA transfer, to submit the required information to individuals who are not obliged entities. VASPs receiving a VA transfer from an entity that is not a VASP or other obliged entity (*e.g.*, from an individual VA user to an unhosted wallet), should obtain the required originator and beneficiary information from their customer. Countries should require their VASPs or other obliged entities to implement mechanisms to ensure effective scrutiny of suspicious activity reporting and to meet the requirements of sanctions implementation (see the discussion of Recommendation 20 below) and as discussed above may choose to impose additional limitations, controls, or prohibitions on unhosted wallets.

~~Recommendation 16 was developed with the objective of preventing terrorists and other criminals from having unfettered access to electronically facilitated funds transfers – which at the time of drafting the FATF termed "wire transfers" – for moving their funds and for detecting such misuse when it occurs. It establishes the requirements for countries relating to wire transfers and related messages and applies to both domestic and cross-border wire transfers. Recommendation 16 defines "wire transfers" as any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.~~

~~In accordance with the functional approach of the FATF Recommendations, the requirements relating to wire transfers and related messages under Recommendation 16 apply to all providers of such services, including VASPs that provide services or engage in activities, such as VA transfers, that are functionally analogous to wire transfers. Countries should apply Recommendation 16 regardless of whether the value of the traditional wire transfer or the VA transfer is denominated in fiat currency or a VA. However, countries may adopt a de minimis threshold for VA transfers of USD/EUR 1 000, having regard to the risks associated with various VAs and covered VA activities.~~

~~Consequently, the requirements of Recommendation 16 should apply to VASPs whenever their transactions, whether in fiat currency or VA, involve: (a) a traditional wire transfer, or (b) a VA transfer or other related message operation between a VASP and another obliged entity (e.g., between two VASPs or between a VASP and another obliged entity,~~

such as a bank or other FI). In the latter scenarios (i.e., transactions involving VA transfers), countries should treat all VA transfers as cross-border wire transfers, in accordance with the Interpretative Note to Recommendation 16 (INR. 16), rather than domestic wire transfers, based on the cross-border nature of VA activities and VASP operations.

As described in INR.15, paragraph 7(b), all of the requirements set forth in Recommendation 16 apply to VASPs or other obliged entities that engage in VA transfers, including the obligations to obtain, hold, and transmit required originator and beneficiary information in order to identify and report suspicious transactions, monitor the availability of information, take freezing actions, and prohibit transactions with designated persons and entities. Countries should therefore ensure that ordering institutions (whether a VASP or other obliged entity such as a FI) involved in a VA transfer obtain and hold required and accurate[42] originator information and required beneficiary information and submit the information to beneficiary institutions (whether a VASP or other obliged entity such as a FI), if any. Further, countries should ensure that beneficiary institutions (whether a VASP or other obliged entity) obtain and hold required (not necessarily accurate) originator information and required and accurate beneficiary information, as set forth in INR. 16. The required information includes the: (i) originator's name (i.e., the sending customer); (ii) originator's account number where such an account is used to process the transaction (e.g., the VA wallet); (iii) originator's physical (geographical) address, or national identity number, or customer identification number (i.e., not a transaction number) that uniquely identifies the originator to the ordering institution, or date and place of birth; (iv) beneficiary's name; and (v) beneficiary account number where such an account is used to process the transaction (e.g., the VA wallet). It is not necessary for the information to be attached directly to the VA transfer itself. The information can be submitted either directly or indirectly, as set forth in in INR. 15.

It is vital that countries ensure that providers of VA transfers – whether VASPs or other obliged entities – transmit the required originator and beneficiary information immediately and securely, particularly given the rapid and cross-border nature of VA transfers and in line with the objectives of Recommendation 16 (as well as the traditional requirement in Recommendation 16 for originator and beneficiary information to "accompany […] wire transfers" involving fiat currency). "Securely" in the context of INR. 15, paragraph 7(b), is meant to convey that providers should protect the integrity and availability of the required information to facilitate recordkeeping (among other requirements) and the use of such information by receiving VASPs or other obliged entities as well as to protect it from unauthorized disclosure. Use of the term is not meant to impede the objectives of Recommendation 16 or Recommendation 9. "Immediately," – also in the context of INR. 15, paragraph 7(b) and given the cross-border nature, global reach, and transaction speed of VAs – means that providers should submit the required information simultaneously or concurrently with the transfer itself. (See Section IV for additional information on these issues specific to VASPs and other obliged entities.)

Countries should require both the ordering and beneficiary institution under their national frameworks to make the above required information available to appropriate authorities upon request. Further, they should require both ordering and beneficiary institutions to take freezing actions and prohibit transactions with designated persons and entities (i.e., screening customers in order to comply with their targeted financial sanctions obligations). Accordingly, the ordering institution should have the required information about its customer, the originator, and the beneficiary institution should have the required

[42] See FATF Glossary of specific terms used in Recommendation 16, wherein "accurate is used to describe information that has been verified for accuracy".

~~information about its customer, the beneficiary, in line with the customer due diligence requirements set forth in Recommendation 10.~~

~~The FATF recognizes that unlike traditional fiat wire transfers, not every VA transfer may involve (or be bookended by) two obliged entities, whether a VASP or other obliged entity such as a FI. In instances in which a VA transfer involves only one obliged entity on either end of the transfer (e.g., when an ordering VASP or other obliged entity sends VAs on behalf of its customer, the originator, to a beneficiary that is not a customer of a beneficiary institution but rather an individual VA user who receives the VA transfer using his/her own distributed ledger technology (DLT) software, such as an unhosted wallet), countries should still ensure that the obliged entity adheres to the requirements of Recommendation 16 with respect to their customer (the originator or the beneficiary, as the case may be). The FATF does not expect that VASPs and financial institutions, when originating a VA transfer, would submit the required information to individual users who are not obliged entities. VASPs receiving a VA transfer from an entity that is not a VASP or other obliged entity (e.g., from an individual VA user using his/her own DLT software, such as an unhosted wallet), should obtain the required originator information from their customer.~~

~~Similarly, there may be VA transfer scenarios, either now or in the near-future, that involve "intermediary VASPs" or other intermediary obliged entities or FIs that facilitate VA transfers as an intermediate element in a chain of VA transfers. Countries should ensure that such intermediary institutions (whether a VASP or other obliged entity) also comply with the requirements of Recommendation 16, as set forth in INR. 15, including the treatment of all VA transfers as cross-border qualifying transfers. Just as a traditional intermediary FI processing a traditional fiat cross-border wire transfer must ensure that all required originator and beneficiary information that accompanies a wire transfer is retained with it, so too must an intermediary VASP or other comparable intermediary institution that facilitates VA transfers ensure that the required information is transmitted along the chain of VA transfers as well as to maintain necessary records and make the information available to appropriate authorities upon request. Intermediary institutions involved in VA transfers also have obligations under Recommendation 16 to identify suspicious transactions, take freezing actions, and prohibit transactions with designated persons and entities just like ordering and beneficiary VASPs (or other ordering or beneficiary obliged entities that facilitate VA transfers).~~

Reliance on third parties

~~84.~~181. **Recommendation 17** allows countries to permit obliged entities to rely on third parties to introduce business and/or perform part of the CDD process, including the identification and verification of customers' identities. The third party, however, must be a regulated entity that the competent authorities supervise and monitor for AML/CFT, with measures in place for compliance with CDD and recordkeeping requirements. In addition, reliance on a third party will not relieve the obliged entity of its obligations or liability in the event of a breach.

182. Countries may permit VASPs to act as third parties, in accordance with their status under Recommendation 15. In addition to checking the regulated status of the third party, obliged entities should conduct their selection on a risk basis. In the context of third-party VASPs, countries and obliged entities should consider the risks potentially posed by the third party, the nature of the business or operation, the third-party VASP's customer groups or target markets, and its business partners, where relevant. Where a VASP relies on another VASP for business introduction or in the conduct of CDD, the VASP-to-VASP reliance for CDD, particularly in the context of VA transfers, should occur in a manner consistent and compliant with the requirements of Recommendation 16.

Internal controls and foreign branches and subsidiaries

183. **Recommendation 18** requires countries to require obliged entities, such as VASPs, to have internal controls in place with a view to establishing the effectiveness of the AML/CFT policies and processes and the quality of the risk management across its operations, departments, branches and subsidiaries, both domestically and, where relevant, abroad. Those internal controls should include appropriate governance arrangements where responsibility for AML/CFT is clearly allocated and a compliance officer is appointed at management level; controls to monitor the integrity of staff, which are implemented in accordance with the applicable local legislation; ongoing training of staff; and an (external or internal) independent audit function to test the system.

Higher risk countries

184. **Recommendation 19** requires countries to require obliged entities, such as VASPs, to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons from higher risk countries, which include countries for which enhanced due diligence measures are called for by the FATF. This is of specific relevance for VA activities and VASPs, given the cross-border nature of their activities.

STRs and tipping-off

~~85.~~185. **Recommendation 20** requires all FIs that suspect or have reasonable grounds to suspect that funds are the proceeds of crime or are related to terrorist financing to report their suspicions promptly to the relevant FIU. Accordingly, countries should ensure that VASPs as well as any other obliged entities that engage in covered VA activities file STRs (see Section IV for additional information specific to VASPs and other obliged entities).

~~86.~~186. Consistent with paragraph 7 of INR. 15 relating to the application of the preventive measures and as discussed above in the context of Recommendation 16, countries also should require VASPs to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate (again, see Section IV for additional information).

187. In some jurisdictions that already implement comprehensive AML/CFT obligations for VASPs and other obliged entities that engage in VA activities, STRs that reference VAs have proven invaluable in furthering law enforcement investigative efforts as well as for improving the FIU's ability to better understand and analyse both providers and activities in the VA ecosystem.[43] Countries should consider whether updates to their existing reporting mechanisms or forms are necessary in order to enable providers or other obliged entities to report specific indicators that may be associated with VA activity, such as device identifiers, IP addresses with associated time stamps, VA wallet addresses, and transaction hashes.

~~87.~~ Although VASPs are not required to submit verified required information on the beneficiary (see Recommendation 16 above), there could be the situation where a VASP has suspicion on the accuracy of data it processes from any discrepancies that the VASP has noted. These discrepancies could be identified with the support from blockchain analytic tools; information provided by its counterparty VASP; external authorities; or based on its transaction history and records. If there are any discrepancies due to the wrong

[43] For example, STRs filed both by depository institutions and VASPs (specifically, exchangers) enabled U.S. law enforcement to take action in 2017 against BTC-e—an Internet-based money transmitter that exchanged fiat currency as well as VAs and facilitated transactions involving ransomware, computer hacking, identity theft, tax fraud schemes, public corruption, and drug trafficking—by helping them to identify VA wallet addresses used by BTC-e and detect different illicit streams of activity moving through the exchange.

information provided by its customer (in case of originator VASPs), or originator VASP (in case of beneficiary VASPs), this could generate some suspicions against a counterparty. Such recognition could be highly valuable information for FIUs, LEAs and investigators. Therefore, jurisdictions should require their VASPs to implement mechanisms to ensure effective scrutiny of STRs and to meet the requirements of sanctions implementation.

188.

~~88.~~189. **Recommendation 21** relates to the tipping-off and confidentiality measures applicable to FIs under the FATF Recommendations. Countries should also apply such measures to VASPs, as set forth in paragraph 7 of INR. 15 relating to the application of the preventive measures. VASPs, their directors, officers, and employees, where applicable, should be protected by law from criminal and civil liability for breach of any restriction on disclosure of information and prohibited by law from disclosing (or "tipping-off") STRs, as detailed in Recommendation 21.

Transparency and Beneficial Ownership of Legal Persons and Arrangements

~~89.~~190. **Recommendations 24 and 25.** The FATF Glossary defines VASPs as *any natural or legal* person that conducts as a business the activities or operations specified in the VASP definition. Recommendations 24 and 25 explicitly note that countries should take measures to prevent the misuse of legal persons and arrangements for money laundering and terrorist financing. As with FIs and DNFBPs, countries should therefore take measures to prevent the misuse of VASPs and consider measures to facilitate access to beneficial ownership and control information by VASPs undertaking the requirements set out in Recommendations 10 and 22.

Operational and Law Enforcement

~~90.~~191. **Recommendation 29.** STRs filed by VASPs (or other obliged entities such as traditional FIs that may be operating in the VA space or engaging in covered VA activities) under Recommendation 20 must be filed with the FIU. Additionally, FIUs should be able to obtain additional information from reporting entities in their jurisdiction, which include VASPs, and should have access on a timely basis to the financial, administrative, and law enforcement information that the FIU requires to undertake its functions properly.

~~91.~~192. Readers of this Guidance should note that **Recommendation 30** is addressed above in the funds- or value-based terms section of the Recommendation-by-Recommendation analysis.

~~92.~~193. **Recommendation 31.** As with FIs and DNFBPs, countries and competent authorities should be able to obtain access to all necessary documents and information, including powers to use compulsory measures for the production of records, held by VASPs. They should have effective mechanisms in place to identify whether natural or legal persons such as VASPs hold or control VA accounts or wallets and mechanisms for ensuring that competent authorities have a process to identify assets, including VAs, without prior notification to the owner. The application of Recommendation 31 is particularly important for countries and their competent authorities in addressing and mitigating the ML/TF risks associated with covered VA activities and VASPs.

~~93.~~194. **Recommendation 32.** Jurisdictions should take a risk-based approach in considering whether to apply Recommendation 32 to covered VA activities and VASPs. Specifically, jurisdictions should consider in their risk-based approach (a) whether the activities of VASPs and with VAs fall under the parameters of transportation of physical monetary instruments and (b) how establishing requirements for declaration and systems

for detection of cross-border movement of such assets would work in practice as well as how they would mitigate ML/TF risks in their jurisdiction.

~~94.~~195. As with Recommendation 30, readers of this Guidance should note that **Recommendation 33** is addressed above in the funds- or value-based terms section.

~~95.~~196. **Recommendation 34** is a vital component in countries' approaches to identifying and addressing the ML/TF risks associated with VA activities and VASPs, as well as in relation to the VAs themselves. The relevant competent authorities should establish guidelines and provide feedback that will assist VASPs (as well as other obliged entities, including traditional FIs) in applying national measures to combat money laundering and terrorist financing and, in particular, in detecting and reporting suspicious transactions—whether virtual/fiat or virtual/virtual.

International Co-operation

~~96.~~197. **Recommendations 36 through 40.** Given the cross-border and mobile nature of VA activities and the VASP sector, international co-operation and the implementation of Recommendations 36 through 40 by countries and competent authorities is critical, particularly the measures applicable to countries and competent authorities in Recommendations 37 through 40. Moreover, effective implementation of the requirements relating to international co-operation is important for limiting the ability of providers' of VA activities in one jurisdiction from having an unfair competitive advantage over providers in other, potentially more regulated, jurisdictions and limit jurisdiction shopping or hopping or regulatory arbitrage.

~~97.~~198. Recognizing that effective regulation, supervision, and enforcement relating to the VASP sector requires a global approach and a level regulatory framework across jurisdictions, paragraph 8 of INR. 15 underscores the importance of the application of Recommendations 37 through 40 for mitigating the risks associated with VAs, covered VA activities, and VASPs. Countries should have in place the tools necessary to co-operate with one another, provide mutual legal assistance (Recommendation 37); help identify, freeze, seize, and confiscate the proceeds and instrumentalities of crime that may take the form of VAs as well as other traditional assets associated with VASP activities (Recommendation 38); and provide effective extradition assistance in the context of VA-related crimes or illicit actors who engage in illicit activities (Recommendation 39), among other international capabilities.

~~98.~~199. As with other Recommendations that include funds- or value-based terms, countries should apply the confiscation and provisional measures relating to "property laundered from, proceeds from, instrumentalities used in, or instrumentalities intended for use in money laundering, predicate offences, or terrorist financing; or property of corresponding value" in the context of VAs.

~~99.~~200. Paragraph 8 of INR. 15 also specifically requests that supervisors of VASPs exchange information promptly and constructively with their foreign counterparts, regardless of the supervisors' nature or status or differences in the nomenclature or status of VASPs (see sub-sections 3.1.4 and 3.18 above).

~~100.~~201. International co-operation is also relevant in the context of VASPs that seek to register or license themselves in one jurisdiction but provide products or services "offshore" to customers located in other jurisdictions. It is important that FIUs co-operate and exchange relevant information on relevant STRs with their counterparts in a timely manner, especially in relation to cross-border VA activities or VASP operations. Sufficient oversight and regulatory control of VASPs operating in their jurisdiction enables countries to better provide investigatory assistance and other international co-operation in the VA

space. At present, the lack of regulation and investigation capacity in most countries may present obstacles to countries' ability to provide meaningful international co-operation. Moreover, many countries do not have legal frameworks that allow them to criminalize certain VA-related ML/TF activities, which could further limit their ability to provide effective mutual legal assistance in situations where dual criminality is required. Authorities should also consider the Principles of Information-Sharing and Co-operation amongst VASP Supervisors for further guidance on how supervisors can co-operate with their counterparts (see Section VI).

DNFBPs that Engage in or Provide Covered VA Activities

~~101.~~202. When a DNFBP engages in VASP activity (*e.g.*, when a casino offers VA-based gaming or engages in other covered VA activities, products, or services), countries should subject the entity to all of the measures for VASPs set forth in the FATF Recommendations. Countries should note, for example, that Recommendations 22 and 23 set out the CDD, recordkeeping, and other requirements for certain types of DNFBPs in the following situations: (a) casinos, (b) real estate agents, (c) dealers in precious metals and stones, (d) lawyers, notaries, other independent legal professionals and accountants, and (e) trust and company service providers. Recommendation 22 specifically notes that the requirements set out in Recommendations 10, 11, 12, 15, and 17 apply to DNFBPs. Thus, in considering how to regulate and supervise and apply the preventive measures to DNFBPs that engage in VASP activities, countries should refer to the application of Recommendations 10, 11, 12, 15, and 17, among other Recommendations relevant to VASPs, and apply the appropriate CDD, recordkeeping, and other measures accordingly.

~~102.~~203. Similarly, Recommendation 28 requires countries and competent authorities to subject DNFBPs to regulatory and supervisory measures, as set out in the FATF Recommendations. As stated previously, countries should subject VASPs, including DNFBPs that engage in VASP activities, to a level of supervision and regulation on par with FIs and not to DNFBP-level supervision. Where a DNFBP engages in covered VASP activities (*e.g.*, a casino that provides VA products and services or engages in covered VA activities), countries should subject the DNFBP to a higher level of supervision (*e.g.*, "DNFBP plus" supervision), consistent with the higher level of supervision for all VASPs, which is equivalent to the level of supervision and regulation for FIs as laid out in Recommendations 26 and 27. In such instances, the entity is, in essence, a VASP engaging in specified financial activities and not a DNFBP, regardless of what a country may term, call, or label such an entity, institution, or product or service provider. This approach by countries will help to ensure a level regulatory playing field across the VASP sector globally and a level of supervision for VASPs that is consistent with and appropriate for the types of activities in which they engage. See Section I above for further information as to who a VASP is.

Risk-Based Approach to Supervision or Monitoring of VASPs

Understanding the ML/TF Risks

204. The risk-based approach to AML/CFT aims to develop prevention or mitigation measures that are commensurate with the ML/TF risks that countries and the relevant obliged entities identify. In the case of supervision, the risk-based approach applies to the way in which supervisory authorities allocate their resources. It also applies to supervisors discharging their functions in a way that is conducive to the application of the risk-based approach by VASPs.

~~103.~~205. In March 2021, the FATF released Guidance for supervisors on the risk-based approach to AML/CFT supervision. This document sets out guidance for supervisors to assist them in undertaking risk-based supervision broadly. It also includes additional guidance and practical advice for VASP supervisors specifically. This document should be read in conjunction with this Guidance here.

~~104.~~206. An effective risk-based regime should reflect a country's policy, legal, and regulatory approach. The national policy, legal, and regulatory framework should also reflect the broader context of financial sector policy objectives that the country is pursuing, including financial inclusion, financial stability, financial integrity, and financial consumer protection goals, and consider such factors as market competition. The extent to which the national framework allows VASPs to apply a risk-based approach should also reflect the nature, diversity, and maturity of the VASP sector and its risk profile as well as the ML/TF risk associated with individual VASPs and specific VA products, services, or activities.

~~105.~~207. Supervisors should also develop a deep understanding of the VASP market, its structure, and its role in the financial system and the country's economy to better inform their assessment of risk in the sector. This may require investing in training, personnel, or other resources that enable supervisors to gain the practical skillsets and expertise needed to regulate and supervise the range of VA providers and activities described in the VA services or business models at the onset of this Guidance.

208. Supervisors should draw on a variety of sources to identify and assess the ML/TF risks associated with VA products, services, and activities as well as with VASPs. Such sources should include, but are not limited to, the jurisdiction's national or sectoral risk assessments, domestic or international typologies and supervisory expertise, and FIU guidance and feedback. Where competent authorities do not adequately understand the VASP sector or broader VA ecosystem in the country, it may be appropriate for competent authorities to undertake a more targeted sectoral risk assessment in relation to the VASP sector and/or VA environment in order to develop a national-level understanding of the relevant ML/TF risks and to inform the institutional assessments that should be undertaken by VASPs.

~~106.~~209. A number of jurisdictions are using, or exploring using, blockchain analytics services to assist with their supervision. The services can be used in a number of ways, including to pinpoint areas that supervisors may wish to focus on during assessments of individual firms and helping to categorise the highest risk firms based on their activity. There is a cost consideration with these tools and not all VAs are covered by all vendors. Blockchain analytics are also widely used by VASPs and some FIs to monitor their own exposure to risk (*e.g.*, VA transfers that have passed through mixer services). It is important to consider any potential implications for privacy and data protection in the use of such tools, if they allow transparency that is not otherwise available (*e.g.*, on public blockchains).

~~107.~~210. Access to information about ML/TF risks is fundamental for an effective risk-based approach. Recommendation 1 (see INR. 1.3) requires countries, including supervisors, to take appropriate steps to identify and assess ML/TF risks for the country on an ongoing basis in order to make information available for AML/CFT risk assessments conducted by FIs and DNFBPs, including VASPs. Countries, including supervisors, should keep the risk assessments up-to-date and should have mechanisms to provide appropriate information on the results to all relevant competent authorities, FIs, and DNFBPs, including VASPs. In situations where some parts of the VASP sector have potentially limited capacity to identify the ML/TF risks associated with VA products, services, or activities, countries, including supervisors, should work with the sector to understand its risks and to help the private sector

in developing its own understanding of the risks. Depending on the capacity of the VASP sector, general information or more granular information and support may be required.

~~108.~~211. In considering individual VASPs or particular VA products, services, or activities, supervisors should take into account the level of risk associated with the VASPs' products and services, business models, corporate governance arrangements, financial and accounting information, delivery channels, customer profiles, geographic location, countries of operation, VASPs' level of compliance with AML/CFT measures, as well as the risks associated with specific VA tokens or products that potentially obfuscate transactions or undermine the ability of VASPs and supervisors to implement effective AML/CFT measures. Supervisors should also look at the controls in place in a VASP, including the quality of a VASP's risk management policy or the functioning of its internal oversight mechanisms. Other information that may be relevant in the AML/CFT context includes the fitness and propriety of the VASP's management and compliance functions.

~~109.~~212. Some of the aforementioned information can be obtained through prudential supervisors in countries where VASPs or other obliged entities that engage in covered VA activities are subject to prudential regulations (*i.e.*, where VASPs are traditional FIs subject to the Core Principles,[44] such as banks, insurance companies, securities providers, or investment companies), which therefore involves appropriate information sharing and collaboration between prudential and AML/CFT supervisors, especially when the responsibilities belong to separate agencies. In other regulatory models, such as those that focus on licensing or registration of VASPs at the national level but have shared oversight and enforcement at the state level, information sharing should include the sharing of examination findings.

~~110.~~213. Where relevant, information from other stakeholders, such as supervisors (including overseas supervisors and supervisors of payment systems and instruments as well as securities, commodities and derivatives thereof), the FIU and law enforcement agencies may also be helpful for supervisors in determining the extent to which a VASP effectively manages the ML/TF risks to which it is exposed. Some regimes, such as those that only require registration (without extensive background testing) may still enable law enforcement and regulators to be aware of the existence of a VASP, its lines of business, its particular VA products or services, and/or its controlling interests.

~~111.~~214. Supervisors should review their assessment of the risk profiles of both the VASP sector and VASPs periodically and when VASPs' circumstances change materially or relevant new threats emerge. Examples of existing country supervisory practices for VASPs or the broader VASP sector as well as country examples relating to ML/TF risks associated with particular VA products, services, or business models can be found in Section V of this Guidance.

Mitigating the ML/TF Risks

~~112.~~215. The FATF Recommendations require supervisors to allocate and prioritize more supervisory resources to areas of higher ML/TF risk. This means that supervisors should determine the frequency and intensity of periodic assessments based on the level of ML/TF risks to which the sector and individual VASPs are exposed. Supervisors should give priority to the potential areas of higher risk, either within the individual VASP (*e.g.*, to the

---

44 Under the FATF Recommendations, "core principles" refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulated issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.

particular products, services, or business lines that a VASP may offer, such as particular VAs or VA services like AECs or mixers and tumblers that may further obfuscate transactions or undermine the VASP's ability to implement CDD measures) or to particular types of VASPs~~VASPs operating in a particular sector~~ (*e.g.*, to VASPs that only or predominantly facilitate virtual-to-virtual financial activities or that offer particular VA obfuscating products or services, or VASPs that facilitate VA transfers on behalf of their customers to individual users that are not customers of another regulated entity, such as a beneficiary institution), or VASPs operating from or in higher-risk jurisdictions. If a jurisdiction chooses to classify an entire sector as higher risk, countries should still understand and be able to provide some explanation and granularity on the categorisation of individual VASPs within the sector based on their customer base, the countries they deal with, and their applicable AML/CFT controls.

~~113.~~216. It is also important that competent authorities acknowledge that in a risk-based regime, not all VASPs will adopt identical AML/CFT controls and that single, unwitting and isolated incidents involving the transfer or exchange of illicit proceeds do not necessarily invalidate the integrity of a VASP's AML/CFT controls. On the other hand, VASPs should understand that a flexible risk-based approach does not exempt them from applying effective AML/CFT controls.

~~114.~~217. Examples of ways in which supervisors can adjust their approach include:

a) *Adjusting the type of AML/CFT supervision or monitoring*: supervisors should employ both offsite and onsite access to all relevant risk and compliance information. However, to the extent permitted by their regime, supervisors can determine the correct mix of offsite and onsite supervision or monitoring of VASPs. Offsite supervision alone may not be appropriate in higher risk situations. However, where supervisory findings in previous examinations (either offsite or onsite) suggest a low risk for ML/TF, resources can be allocated to focus on higher risk VASPs. In that case, lower risk VASPs could be supervised offsite, for example through transaction analysis and questionnaires.

b) *Adjusting the frequency and nature of ongoing AML/CFT supervision or monitoring*: supervisors should adjust the frequency of AML/CFT examinations in line with the risks identified and combine periodic reviews and ad hoc AML/CFT supervision as issues emerge (*e.g.*, as a result of credible whistleblowing, information from law enforcement, analysis of financial reporting or other supervisory findings). Other risk-based approaches to supervision could include consideration of the geographic location, registration or licensing status, customer base, transaction type (*e.g.*, virtual/fiat or virtual/virtual transactions), VA type, number of accounts or wallets, revenue, products or services offered (*e.g.*, more transparent services versus those products or services that obfuscate transactions, such as AECs), prior history of non-compliance, and/or significant changes in management.

c) *Adjusting the intensity of AML/CFT supervision or monitoring and reporting requirements*: supervisors should decide on the appropriate scope or level of assessment in line with the risks identified, with the aim of assessing the adequacy of VASPs' policies and procedures that are designed to prevent VASPs' abuse. Examples of more intensive supervision could include detailed testing of systems and files to verify the implementation and adequacy of the VASPs' risk assessment, reporting and recordkeeping policies and processes, internal auditing, interviews with operation staff, senior management and the Board of Directors, where applicable.

~~115.~~218. Supervisors should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT

supervision and AML/CFT rules and guidance remains adequate. Whenever appropriate, and in compliance with any relevant standards or requirements relating to the confidentiality of such information, supervisors should communicate their findings to VASPs to enable them to enhance the quality of their risk-based approaches.

General Approach

~~116.~~219. Supervisors should understand the ML/TF risks faced by VASPs or associated with the VASP sector. Supervisors should have a comprehensive understanding of higher and lower risk lines of business or particular VA products, services or activities, with a particularly thorough understanding of the higher-risk products, services or activities.

~~117.~~220. Supervisors should ensure that their staff is trained and equipped to assess whether a VASP's policies, procedures, and controls are appropriate and proportional in view of the VASP's risk assessment and risk management procedures. To support supervisors' understanding of the overall strength of measures in the VASP sector, countries could consider conducting a comparative analysis of VASPs' AML/CFT programs in order to further inform their judgment of the quality of an individual VASP's controls.

~~118.~~221. In the context of the risk-based approach, supervisors should determine whether a VASP's AML/CFT compliance and risk management program is adequate to (i) meet the regulatory requirements, and (ii) appropriately and effectively mitigate and manage the relevant risks. In doing so, supervisors should take into account the VASP's own risk assessment. In the case of VASPs that operate across different jurisdictions on the basis of multiple licenses or registrations, given the cross-border nature of covered VA activities, the supervisor that licenses or registers the natural or legal person VASP should take into consideration the risks to which the VASP is exposed and the extent to which those risks are adequately mitigated.

222. As part of their examination procedures, supervisors should communicate their findings and views about an individual VASP's AML/CFT controls and communicate clearly their expectations of the measures needed for VASPs to comply with the applicable legal and regulatory frameworks. In jurisdictions where VA financial activities may implicate multiple competent authorities, supervisory counterparts within the jurisdiction should also co-ordinate with one another, where applicable, to effectively and clearly communicate their expectations to VASPs as well as to other obliged entities that may engage in VA activities or provide VA products or services. This is particularly important in the context of VASPs that engage in various types of regulated VA activity (*e.g.*, VA money or value transfer services or securities, commodities or derivatives activity) or in VA financial activities that may implicate various banking, securities, commodities, or other regulators.

223. Where AML/CFT weaknesses are identified in VASPs, supervisors should follow-up and assess the robustness of remediation actions taken to rectify the deficiencies, and to prevent recurrence. For regulatory breaches, supervisors should have a broad range of regulatory/supervisory measures available that can be applied to address the risks exposed by the lack of compliance. This range could include warnings, action letters, orders, agreements, administrative sanctions, penalties and fines and other restrictions and conditions on a VASP's activities. A full range of measures should be applied taking into account the level of severity of the identified breaches in the context of unmitigated risks. Priority should be given to those deficiencies that expose the system to the greatest ML/TF risks. For further guidance on applying dissuasive, proportionate and effective sanctions, see the FATF's Guidance on Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement.

224. VASPs or FIs involved in so-called stablecoins, should be supervised in the same manner as VAs or traditional financial assets as appropriate. Like other VAs, assessment of their risks should form part of this process, and so-called stablecoins may tend to pose higher risks, according to the judgement of supervisors, with attendant consequences for the type and intensity of supervision. If a given so-called stablecoin qualifies as a traditional financial asset, it should be supervised according to that determination in the same manner as all other similarly categorized assets. Given the cross-border nature of VA transfers, international cooperation of VASP supervisors is very important.

Guidance

~~119.~~225. Supervisors should communicate their expectations of VASPs' compliance with their legal and regulatory obligations and may consider engaging in a consultative process, where appropriate, with relevant stakeholders. Such guidance may be in the form of high-level requirements based on desired outcomes, risk-based obligations, and information about how supervisors interpret relevant legislation or regulation or more detailed guidance about how VASPs might best apply particular AML/CFT controls.

~~120.~~226. Supervisors and other competent authorities may consider the guidance and input of VA technical experts in order to develop a deeper understanding of the relevant business models and operations of VASPs, their potential exposure to ML/TF risks, as well as the ML/TF risks associated with particular VA types or specific covered VA activities and to make an informed judgment about the mitigation measures in place or needed.

~~121.~~227. As discussed previously, providing guidance for and feedback to the VASP sector is essential and is a requirement under Recommendation 34. The guidance could include best practices that enable VASPs to undertake assessments and develop risk mitigation and compliance management systems to meet their legal and regulatory obligations. Supporting ongoing and effective communication between supervisors and VASPs is an essential component of the successful implementation of a risk-based approach.

~~122.~~228. Supervisors of VASPs should also consider liaising with other relevant domestic regulatory and supervisory authorities to secure a coherent interpretation of VASPs' legal obligations and to promote a level playing field, including between VASPs and between VASPs and other obliged entities such as FIs and DNFBPs. Such co-ordination is particularly important where more than one supervisor is responsible for supervision (*e.g.*, where the prudential supervisor and the AML/CFT supervisors are in different agencies or in separate divisions of the same agency). It also is particularly relevant in the context of VASPs that provide various products or services or engage in different financial activities that may fall under the purview of different regulatory or supervisory authorities within a particular jurisdiction. Multiple sources of guidance should not create opportunities for regulatory arbitrage, loopholes, or unnecessary confusion among VASPs. When possible, relevant regulatory and supervisory authorities in a jurisdiction should consider preparing joint guidance.

Training

~~123.~~229. Training is important for supervision staff to understand the VASP sector and the various business models that exist. In particular, supervisors should ensure that staff are trained to assess the quality of a VASP's ML/TF risk assessment and to consider the adequacy, proportionality, effectiveness, and efficiency of the VASP's AML/CFT policies, procedures, and internal controls in light of its risk assessment. Training in blockchain or other analytics may also be useful.

~~124.~~230. Training should allow supervisory staff to form sound judgements about the quality of the VASP's risk assessments and the adequacy and proportionality of a VASP's AML/CFT controls. It should also aim at achieving consistency in the supervisory approach at a national level in cases where there are multiple competent supervisory authorities or when the national supervisory model is devolved or fragmented.

~~125.~~231. Similarly, countries should consider opportunities for public-private sector training and collaboration to further educate and raise awareness among both operational and other competent authorities and industry on various issues relating to VAs and VASP activities.

Information Exchange

~~126.~~232. Information exchange between the public and private sector is important and should form an integral part of a country's strategy for combating ML/TF in the context of VA and VASP activities. Public authorities should share risk information, where possible, to better help inform the risk assessments of VASPs. The type of information relating to risks in the VA space that the public and private sectors could share include:

a) ML/TF risk assessments;

b) Typologies and methodologies of how money launderers or terrorist financiers misuse VASPs, a particular VA mechanism over another (*e.g.*, VA transfer or exchange activities versus VA issuance activities in the context of money laundering or terrorist financing) or VAs more generally;

c) General feedback on the quality and usefulness of STRs and other relevant reports;

d) Information on suspicious indicators associated with VA activities or VASP transactions;

e) Targeted unclassified intelligence, where appropriate and subject to the relevant safeguards such as confidentiality agreements; and

f) Countries, persons, or organisations whose assets or transactions should be frozen pursuant to targeted financial sanctions as required by Recommendation 6.

~~127.~~233. Further, countries should consider how they might share information with the private sector in order to help the private sector, including VASPs, better understand the nature of law enforcement information requests or other government requests for information or to help shape the nature of the requests so that VASPs can provide more accurate and specific information, where applicable, to competent authorities.

~~128.~~234. Domestic co-operation and information exchange between the supervisors of the banking, securities, commodities, and derivatives sectors and the VASP sector; among law enforcement, intelligence, FIU and VASP supervisors; and between the FIU and the supervisor(s) of the VASP sector are also of vital importance for effective monitoring and supervision of VASPs.

~~129.~~235. Similarly, in line with Recommendation 40, cross-border information sharing by authorities and the private sector with their international counterparts is critical in the VASP sector, taking into account the cross-border nature and multi-jurisdictional reach of VASPs. Authorities should also consider the Principles of Information-Sharing and Co-operation amongst VASP Supervisors for further guidance on how to co-operate with their counterparts (see Section VI).

Section IV – Application of FATF Standards to VASPs and other obliged entities that Engage in or Provide Covered VA Activities

236. The FATF Recommendations apply both to countries as well as to VASPs and other obliged entities that provide covered VA-related services or financial activities or operations ("other obliged entities"), including banks, securities broker-dealers, and other FIs. Accordingly, Section IV provides additional guidance specific to VASPs and other obliged entities that may engage in covered VA activities.

~~130.~~237. In addition to identifying, assessing, and taking effective action to mitigate their ML/TF risks, as described under **Recommendation 1**, VASPs and other obliged entities in particular should apply all of the preventive measures in Recommendations 9 through 21 as set forth above in Section III, including in the context of CDD, when engaging in any covered VA activities. Similarly, DNFBPs should be aware of their AML/CFT obligations when engaging in covered VA activities as set forth in INR. 15 and as described in *sub-section 3.1.9.*

238. Readers of this Guidance should note that the below paragraphs relating to individual preventive measures and FATF Recommendations are intended to provide additional specific guidance for VASPs and other obliged entities on certain issues. The lack of a dedicated paragraph for each FATF Recommendation within the preventive measures, as provided in Section III, for example, does not mean that the respective Recommendations or preventive measures contained therein do not also apply to VASPs and other obliged entities that engage in or provide VA activities.

239. In general, the preventive measures set out in Recommendation 10 to 21 apply to VASPs in the same manner as FIs, with two specific qualifications. Firstly, the occasional transaction decimated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000 (rather than USD/EUR 15 000). Secondly, the wire transfer rules set out in Recommendation 16 apply to VASPs and VA transfers in a modified form (the 'travel rule'). This is explained in more detail below.

Customer due diligence

240. **Recommendation 10** sets forth the required CDD measures that FIs must implement for all customers, including identifying the customer and verifying the customer's identity using reliable, independent source documents, data or information; identifying the beneficial owner; understanding and obtaining information on the purpose and intended nature of the business relationship; and conducting ongoing due diligence on the relationship and scrutiny of transactions.

When to conduct CDD

~~131.~~241. Recommendation 10 also describes the scenarios under which FIs must undertake CDD measures, including in the context of establishing business relations, carrying out occasional transactions above the designated threshold (USD/EUR 1 000 for VA transactions), carrying out occasional transactions that are wire transfers as set forth under Recommendation 16 and its Interpretive Note (also USD/EUR 1 000 for VA transfers), where there is a suspicion of ML/TF, or when the FI doubts the veracity or adequacy of previously obtained customer identification data. While countries may adopt a *de minimis* threshold of USD/EUR 1 000 under their national framework for VA transactions that they deem are occasional (as described in Section III) or for VA transfers, all of which are treated as cross-border qualifying wire transfers for the purposes of applying Recommendation 16, it should be underscored that banks, broker-dealers, and other FIs must still adhere to their

respective CDD thresholds when engaging in covered VA activities. For DNFBPs, such as casinos, that engage in covered VA activity, they should apply the *de minimis* threshold of USD/EUR 1 000 for occasional transactions and for occasional transactions that are wire transfers as described in Section III and as discussed below. As noted in Section III in the context of countries, VASPs, in establishing their operating procedures and processes when accepting customers and facilitating transactions, should consider how they can determine and ensure that transactions are in fact only conducted on a one-off or occasional basis rather than on a more consistent (*i.e.*, non-occasional) basis.

242. Although the designated thresholds above which casinos and dealers in precious metals and stones must conduct CDD for occasional transactions and for occasional transactions that are wire transfers are USD/EUR 3 000 and USD/EUR 15 000 respectively, when DNFBPs engage in any covered VA or VASP activities, they are subject to the CDD standards as set forth under INR. 15 (*i.e.*, a *de minimis* threshold of USD/EUR 1 000 for occasional transactions and for occasional transactions that are wire transfers).

How to conduct CDD

~~132.~~243. Regardless of the nature of the relationship or VA transaction, VASPs and other obliged entities should have in place CDD procedures that they effectively implement and use to identify and verify on a risk basis the identity of a customer, including when establishing business relations with that customer; where they have suspicions of ML/TF, regardless of any exemption of thresholds; and where they have doubts about the veracity or adequacy of previously obtained identification data.

~~133.~~244. Like other obliged entities, in conducting CDD to fulfil their obligations under Recommendation 10, VASPs should obtain and verify the customer identification/verification information required under national law. Typically, required customer identification information includes information on the customer's name and further identifiers such as physical address, date of birth, and a unique national identifier number (*e.g.*, national identity number or passport number). Depending upon the requirements of their national legal frameworks, VASPs are also encouraged to collect additional information to assist them in verifying the customer's identity when establishing the business relationship (*i.e.*, at onboarding); authenticate the identity of customers for account access; help determine the customer's business and risk profile and conduct ongoing due diligence on the business relationship; and mitigate the ML/TF risks associated with the customer and the customer's financial activities. Such additional, non-core identity information, which some VASPs currently collect, could include, for example an IP address with an associated time stamp; geo-location data; device identifiers; VA wallet addresses; and transaction hashes.

245. For covered VA activities, the verification of customer and beneficial ownership information by VASPs should be completed before or during the course of establishing the relationship.[45]

246. Where VASP cannot apply the appropriate level of CDD, Recommendation 10 requires the VASP to not enter into a business relationship or carry out an occasional transaction or to terminate an already-existing business relationship; and consider making a STR in relation to the customer.

~~134.~~

[45] *See also* 2015 VC Guidance, paragraph 45.

~~135.~~247. Based on a holistic view of the information obtained in the context of their application of CDD measures—which could include both traditional information and non-traditional information as described above—VASPs and other obliged entities should be able to prepare a customer risk profile in appropriate cases. A customer's profile will determine the level and type of ongoing monitoring potentially necessary and support the VASP's~~'~~ decision whether to enter into, continue, or terminate the business relationship. Risk profiles can apply at the customer level (*e.g.*, nature and volume of trading activity, origin of virtual funds deposited, etc.) or at the cluster level, where a cluster of customers displays homogenous characteristics (*e.g.*, clients conducting similar types of VA transactions or involving the same VA). VASPs should periodically update customer risk profiles of business relationships in order to apply the appropriate level of CDD.

248. If a VASP uncovers VA addresses that it has decided not to establish or continue business relations with or transact with due to suspicions of ML/TF, the VASP should consider making available its list of "blacklisted wallet addresses," subject to the laws of the VASP's jurisdiction. A VASP should screen its customer's and counterparty's wallet addresses against such available blacklisted wallet addresses as part of its ongoing monitoring. A VASP should make its own risk-based assessment and determine~~d~~ whether additional mitigating or preventive actions are warranted if there is a positive hit.

249. VASPs and other obliged entities that engage in covered VA activities may adjust the extent of CDD measures, to the extent permitted or required by their national regulatory requirements, in line with the ML/TF risks associated with the individual business relationships, products or services, and VA activities, as discussed above under the application of Recommendation 1. VASPs and other obliged entities must therefore increase the amount or type of information obtained or the extent to which they verify such information where the risks associated with the business relationship or VA activities is higher, as described in Section III. Similarly, VASPs and other obliged entities may also simplify the extent of the CDD measures where the risk associated with the business relationship of activities is lower. However, VASPs and other obliged entities may not apply simplified CDD or an exemption from the other preventive measures simply on the basis that natural or legal persons carry out the VA activities or services on an occasional or very limited basis (INR. 1.6(b)). Further, simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing or where specific higher-risk scenarios apply (see Section III for an explanation of potentially higher-risk situations)

Ongoing CDD and monitoring

~~136.~~250. Ongoing monitoring on a risk basis means scrutinizing transactions to determine whether those transactions are consistent with the VASP's (or other obliged entity's) information about the customer and the nature and purpose of the business relationship, wherever appropriate. Monitoring transactions also involves identifying changes to the customer profile (*e.g.*, the customer's behaviour, use of products, and the amounts involved) and keeping it up-to-date, which may require the application of enhanced CDD measures. Monitoring transactions is an essential component in identifying transactions that are potentially suspicious, including in the context of VA transactions. Transactions that do not fit the behaviour expected from a customer profile, or that deviate from the usual pattern of transactions, may be potentially suspicious.

~~137.~~251. Monitoring should be carried out on a continuous basis and may also be triggered by specific transactions. Where large volumes of transactions occur on a regular basis, automated systems may be the only realistic method of monitoring transactions, and flagged transactions should go through human/expert analysis to determine if such

transactions are suspicious. VASPs and other obliged entities should understand their operating rules, verify their integrity on a regular basis, and check that they account for the identified ML/TF risks associated with VAs, products or services or VA financial activities.

~~138.~~252. VASPs and other obliged entities should adjust the extent and depth of their monitoring in line with their institutional risk assessment, their ~~and~~ individual customer risk profiles including the type of transactions that they allow (e.g. transactions to/from unhosted wallets, or from/to a wallet that has previously carried out P2P transactions). VASPs may consider choosing to limit or prohibit transactions with unhosted wallets in this regard. Enhanced monitoring should be required for higher-risk situations (as described in Sections II and III) and extend beyond the immediate transaction between the VASP or its customer or counterparty. The adequacy of monitoring systems and the factors that lead VASPs and other obliged entities to adjust the level of monitoring should be reviewed regularly for continued relevance to their AML/CFT risk programme.

253. Monitoring under a risk-based approach allows VASPs or other obliged entities to create monetary or other thresholds to determine which activities will be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine their adequacy for the risk levels established. VASP and other obliged entities should document and state clearly the criteria and parameters used for customer segmentation and for the allocation of a risk level for each of the clusters of customers, where applicable. The criteria applied to decide the frequency and intensity of the monitoring of different customer (or even VA product) segments should also be transparent. To this end, VASPs and other obliged entities should properly document, retain, and communicate to the relevant personnel and national competent authorities the results of their monitoring as well as any queries raised and resolved.

Politically exposed persons

254. **Recommendation 12.** For domestic PEPs[46] and international organisation PEPs,[47] obliged entities, such as VASPs, must take reasonable measures to determine whether a customer or beneficial owner is a domestic or international organisation PEP and then assess the risk of the business relationship. For higher-risk business relationships with domestic PEPs and international organisation PEPs, VASPs and other obliged entities should take additional measures consistent with those applicable to foreign PEPs, including identifying the source of wealth and source of funds when relevant.[48]

Correspondent banking and other similar relationships

255. **Recommendation 13.** "Correspondent banking" does not include one-off transactions (see Recommendation 13 in the Section III), but rather is characterised by its on-going, repetitive nature. VASPs should establish their control framework, by defining and assessing the characteristics of their counterparty VASP relationships and whether they are undertaking activities similar to correspondent banking. This should include

46 "Domestic PEPs" are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials (FATF Glossary).

47 "Persons who are or have been entrusted with a prominent function by an international organisation" refers to members of senior management, *i.e.*, directors, deputy directors, and members of the board or equivalent functions (FATF Glossary).

48 Further information on PEPs is set out in the 2013 FATF *Guidance on Politically Exposed Persons (Recommendations 12 and 22)*.

considering their competent authorities' views on any identified high risk counterparty VASP relationships. Further information on the counterparty VASP due diligence process is set out in Recommendation 16.

Wire transfers and the 'travel rule'

256. **Recommendation 16.** As noted in Section III, providers in this space must comply with the requirements of Recommendation 16 (i.e. the 'travel rule'). This includes the obligation to obtain, hold, and submit required originator and beneficiary information associated with VA transfers in order to identify and report suspicious transactions, take freezing actions, and prohibit transactions with designated persons and entities. The requirements apply to both VASPs and other obliged entities such as FIs when they send or receive VA transfers on behalf of a customer.

Data submission technology, inter-operability and scalability of infrastructure

257. The FATF is technology-neutral and does not prescribe a particular technology or software approach that providers should deploy to comply with Recommendation 16. As noted previously, any technology or software solution is acceptable, so long as it enables the ordering and beneficiary institution (where present in the transaction) to comply with its AML/CFT obligations. For example, a solution for obtaining, holding, and transmitting the required information (in addition to complying with the various other requirements of Recommendation 16) could be code that is built into the VA transfer's underlying DLT transaction protocol or that runs on top of the DLT platform (*e.g.*, using a smart contract, multiple-signature, or any other technology); an independent (*i.e.*, non-DLT) messaging platform or application program interface (API); or any other effective means for complying with the Recommendation 16 measures.

258. These technological solutions should enable VASPs to comply with the travel rule in an effective and efficient manner if they enable a VASP to carry out the following main actions:

a) enable a VASP to locate counterparty VASPs for VA transfers;

b) enable the submission of required and accurate originator and required beneficiary information immediately when a VA transfer is conducted on a DLT platform;

c) enable VASPs to submit a reasonably large volume of transactions to multiple destinations in an effectively stable manner;

d) enable a VASP to securely transmit data, i.e. protect the integrity and availability of the required information to facilitate record-keeping;

e) protect the use of such information by receiving VASPs or other obliged entities as well as to protect it from unauthorized disclosure in line with national privacy and data protection laws;

f) provide a VASP with a communication channel to support further follow-up with a counterparty VASP for the purpose of:

- due diligence against counterparty VASP; and
- requesting information on a certain transaction to determine if the transaction is involving high risk or prohibited activities.

5.

259. VASPs or other obliged entities should implement mechanisms to ensure effective scrutiny of STRs, taking account of the information obtained through the above

communication infrastructure. This could be done by combining other customer information, transaction history, and additional transaction data that it or its counterparty VASP obtained from its customer. VASPs should also ensure that they are screening transactions to meet their sanctions obligations. Further information on this process is set out in the discussion of Recommendation 16 in Section III of this Guidance. When VASPs or other obliged entities consider selecting a technological solution for compliance with the travel rule, they should consider the above control needs.

~~139.~~260. VASPs and other obliged entities in VA transfers, whether as an ordering or beneficiary institution, should consider how they might leverage existing commercially available technology to comply with the requirements of Recommendation 16, and specifically the requirements of INR. 15, paragraph 7(b). Examples of existing technologies that providers could consider as a foundation for enabling the identification of beneficiaries of VA transfers as well as the transmission of required originator and beneficiary in near real-time before a VA transfer is conducted on a DLT platform include:

a) *Public and private keys*, which are created in pairs for each entity involved in a transmission and encrypt and decrypt information during the initial part of the transmission so that only the sender and recipient of the transmission can decrypt and read the information, wherein the public key is available to everyone while the private key is known only to the creator of the keys;

b) *Transport Layer Security/Secure Sockets Layer (TLS/SSL) connections*, which make use of public and private keys among parties when establishing a connection and secure almost all transmissions on the Internet, including emails, web browsing, logins, and financial transactions, ensuring that all data that passes between a web server and a browser remains private and secure;

c) *X.509 certificates*, which are digital certificates administered by certificate authorities that use the X.509 PKI standard to verify that a public key belongs to the user, computer, or service identity in the certificate and which are used worldwide across public and private sectors;

d) *X.509 attribute certificates*, which can encode attributes (such as name, date of birth, address, and unique identifier number), are attached cryptographically to the X.509 certificate, and are administered by attribute certificate authorities;

e) *API technology*, which provides routines, protocols, and tools for building software applications and specifies how software components should interact; as well as

f) Other commercially available technology or potential software or data sharing solutions.

Counterparty VASP identification and due diligence

261. Not all VASPs are the same. They vary in size from small independent business to large multinational corporations. Similarly, no country's AML/CFT regime for VASPs is exactly the same and countries are introducing their measures at different paces. Different entities within a sector will pose higher or lower risks depending on a variety of factors, including products, services, customers, geography and the strength of the entity's compliance program. VASPs should analyse and seek to understand how the ML/TF risks they identify affect them and take appropriate measures to mitigate and manage those risks. The risk assessment, therefore, provides the basis for the risk-based application of AML/CFT measures. As long as global implementation of the FATF Standards on VASPs remains lacking, managing these kinds of relationships will pose a continuing challenge. This underscores the importance of implementation and suggests that VASPs will have to

consider additional control measures for countries with weak implementation, such as intensive monitoring of transactions with VASPs based in the country, placing amount restrictions on transactions, or intensive and frequent due diligence. Otherwise, the VASP may face a tough decision in whether to deal with VASPs based in that country. VASPs and FIs should consider this Guidance in conjunction with the FATF Guidance on Correspondent Banking Services. Although a counterparty VASP relationship may not be a correspondent banking relationship, there are similarities in the approach to counterparty due diligence which can be of assistance to VASPs. Accordingly, the process set out in Recommendation 13 is referenced in this Guidance.

262. When establishing a new counterparty VASP relationship, a VASP may obtain information set out by Recommendations 10 and 13 directly from the counterparty VASP. Under the requirements of those Recommendations, this information should be verified. Examples of potential reliable, independent sources of information for the verification of the identity and beneficial ownership of legal persons and arrangements include: corporate registries, registries maintained by competent authorities on the creation or regulated institutions list (e.g. VASP lists maintained by each jurisdictions where available), registries of beneficial ownership and other examples mentioned in the BCBS General Guide on Account Opening.[49]

263. Some examples of potential sources of information on level of risks include, but are not limited to: the AML/CFT laws and regulations of the home country or the host country where the respondent institution is doing business and how they apply, public databases of legal decisions and/or regulatory or enforcement actions, annual reports that have been filed with a stock exchange, country assessment reports or other information published by international bodies which measure compliance and address ML/TF risks (including the FATF, FSRBs, BCBS, IMF and World Bank), lists issued by the FATF in the context of its International Co-operation Review Group process, reputable newspapers, journals or other open source electronic media, third party databases, national or supranational risk assessments, information from the respondent institution's management and compliance officer(s) and public information from the regulator and supervisor.

264. The VASP should assess the counterparty VASP's AML/CFT controls, similar to the process set out in FATF Recommendation 13, sub-paragraph (b)[50]. In practice, such an assessment should involve reviewing the counterparty's AML/CFT systems and controls framework. The assessment should include confirming that the counterparty's AML/CFT controls are subject to independent audit (which could be external or internal).

265. For clarity, a VASP needs to undertake counterparty VASP due diligence before they transmit the required information for compliance with paragraph 7(b) of INR.15 to their counterparty. VASPs do not need to undertake the counterparty VASP due diligence process for every VA transfer, but should refresh their counterparty due diligence information periodically or when risk emerges from the relationship in line with the risk-based approach controls defined by the VASP.

Submission of required information

266. As set forth in INR. 15, paragraph 7(b), it is vital that VASPs and other obliged entities that engage in VA transfers submit the required information in a secure manner, so as to protect the customer information associated with the VA transfers against unauthorized disclosures and enable receiving entities to effectively comply with their own AML/CFT obligations, including identifying suspicious VA transfers, taking freezing

[49] Annex 4, General guide to account opening, https://www.bis.org/bcbs/publ/d505.htm.

[50] One of the tools that could be used as a starting point to refer is the Wolfsberg questionnaire.

actions, and prohibiting transactions with designated persons and entities. Further~~, and as highlighted in Section III,~~ it is essential that providers submit the required information immediately—that is, simultaneously or concurrent with the transfer itself—particularly given the cross-border nature, global reach, and transaction speed of VA activities. See the discussion of the travel rule in Section III for further information.

267. VASPs must transmit relevant originator and beneficiary information as set out in the INR. 16. Countries may adopt a *de minimis* threshold for VA transfers, below which verification of the customer and beneficiary information is not required unless there is a ML/TF suspicion. That is, for occasional VA transfers below USD/EUR 1 000, or the equivalent amount in local currency, or per defined in local regulations, the requirements of the INR.16 apply and the name of the originator and of the beneficiary will be requested, as well as a wallet address for each or a unique transaction reference number. However, such information will not have to be verified unless there are suspicious circumstances related to ML/TF, in which case information pertaining to the customer should be verified.

Internal controls and foreign branches and subsidiaries

~~6.~~

~~140.~~268. **Recommendation 18.** The successful implementation and effective operation of a risk-based approach to AML/CFT depends on strong senior management leadership, which includes oversight of the development and implementation of the risk-based approach across the VASP sector. Recommendation 18 also requires information sharing within the group, where relevant, regarding in particular unusual transactions or activities.

269. VASP and other obliged entities should maintain AML/CFT programmes and systems that are adequate to manage and mitigate their risks. The nature and extent of the AML/CFT controls will depend upon a number of factors, including the nature, scale and complexity of the VASP's business, the diversity of its operations, including geographical diversity, its customer base, product and activity profile, and the degree of risk associated with each area of its operations, among other factors.

STR reporting and tipping-off

~~141.~~270. **Recommendation 20.** VASPs and other obliged entities that engage in or provide VA activities, products, and services should have the ability to flag for further analysis any unusual or suspicious movements of funds or transactions—including those involving or relating to VAs—or activity that is otherwise indicative of potential involvement in illicit activity regardless of whether the transactions or activities are fiat-to-fiat, virtual-to-virtual, fiat-to-virtual, or virtual-to-fiat in nature. VASPs and other obliged entities should have appropriate systems so that such funds or transactions are scrutinised in a timely manner and a determination can be made as to whether funds or transactions are suspicious.

~~142.~~271. VASPs and other obliged entities should promptly report funds or transactions, including those involving or relating to VAs and/or providers that are suspicious to the FIU and in the manner specified by competent authorities. The processes that VASPs and other obliged entities put in place to escalate their suspicions and ultimately report to the FIU should reflect this. While VASPs and other obliged entities can apply the policies and processes that lead them to form a suspicion on a risk-sensitive basis, they should report their ML/TF suspicions once formed and regardless of the amount of the transaction or whether the transaction has completed. The obligation for VASPs and other obliged entities to report suspicious transactions is therefore not risk-based, nor does the act of reporting discharge them from their other AML/CFT obligations. Further, VASPs and other obliged

entities should comply with applicable STR requirements even when operating across different jurisdictions.

272. Consistent with INR. 15 and in relation to Recommendation 16, in the case of a VASP (or other obliged entity) that controls both the ordering and the beneficiary side of a VA funds or wire transfer, the VASP or other obliged entity should take into account all of the information from both the ordering and beneficiary sides in order to determine whether the information gives rise to suspicion and, where necessary, file an STR with the appropriate FIU and make relevant transaction information available to the FIU. The lack of required originator or beneficiary information should be considered as a factor in assessing whether a transfer involving VAs or VASPs is suspicious and whether it is thus required to be reported to the FIU. The same holds true for other obliged entities such as traditional FIs involved in a transfer involving VAs or VASPs.

273. Where the VASP requests further information on a counterparty or information from its customer in case the VASP receiving a VA transfer from an entity that is not a VASP or other obliged entity, it expects their customer to respond in a timely fashion and provide documents/information to the level of detail requested. Where their customer does not answer, it may trigger concerns for a VASP on their customer being unable to reasonably explain the soundness of its transaction and lead the VASP to consider the filing of a STR on their customer. A request for information could be followed by a reassessment of the customer's attributes and risk profile when necessary.

274. Further information on red-flag indicators for VAs that could suggest criminal behaviour are set out in the FATF's *Virtual Asset Red Flag Indicators of Money Laundering and Terrorist Financing*. These indicators help VASPs and other AML-CFT obliged entities to detect and report suspicious transactions involving VAs. Key indicators include:

a) Technological features that increase anonymity - such as the mixers, tumblers or AECs;

b) Geographical risks - criminals can exploit countries with weak, or absent, national measures for VAs;

c) Transaction patterns – including transactions which are structured to avoid reporting or appear irregular, unusual or uncommon which can suggest criminal activity;

d) Transaction size – if the amount and frequency has no logical business explanation;

e) Sender or recipient profiles - unusual behaviour can suggest criminal activity; and

f) Source of funds or wealth - which can relate to criminal activity.

Section V – Country Examples of Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers

Summary of Jurisdictional Approaches to Regulating and Supervising VA Activities and VASPs

~~143.~~275. Section V provides an overview of various jurisdictional approaches to regulating and supervising VA financial activities and related providers, including approaches to having in place tools and other measures for sanctioning or taking enforcement actions against persons that fail to comply with their AML/CFT obligations, which countries might consider when developing or enhancing their own national frameworks. These countries have not yet been assessed for their compliance with the requirements set forth in INR. 15.

Italy

276. In Italy, Legislative Decree No. 231 of 2007, amended by Legislative Decrees No. 90 of 2017 and No. 125/2019, includes providers engaged in the five functional activities as defined by the FATF, as recipients of the AML/CFT obligations.

~~144. In Italy, Decree No. 231 of 2007, amended by Legislative Decree No. 90 of 2017, includes providers engaged in exchange services between VA and fiat currencies (*i.e.*, "virtual currency exchangers") within the category of subjects obliged to comply with the AML/CFT requirements.~~

~~145.~~277. Service providers related to VAs are required to be listed in a special section of the register held by "*Organismo degli Agenti e dei Mediatori*" (OAM). The registration is a precondition for service providers related to VAs in order to carry out their activity in Italy. Work is currently ongoing to implement the register.

~~146.~~278. VASPs are considered obliged entities and are subject to the full set of AML/CFT measures.

~~147.~~279. On March 21, 2019, Italy adopted the update of the National Risk Assessment (NRA). It includes an assessment of the ML/TF risks emanating from VAs. The results of the updated NRA will be used in order to strengthen the national strategy. Obliged entities and subjects (financial and non-financial) are requested to take into consideration the results of the updated NRA in order to conduct/update their risk assessment.

~~148.~~280. The STRs and the further analysis conducted by the Italian FIU (UIF) permit it to collect information about: i) VASPs operating in Italy, including business data (typology of service provided); location; data on the beneficial owner, administrator and other connected subjects; ii) detailed information on single transactions (*e.g.*, date, amount, executor, counterparts, and wallet accounts); data on the bank accounts involved (*e.g.*, holder, power of attorney, origin/use of the funds, and general features of the financial flows); iii) data on the personal and economic profile of the customer or the holder of the wallet; information useful to match VA addresses to the identity of the owner of the VAs; unambiguous identification data (*e.g.*, fiscal code and VAT number); iv) wallet or account information (*e.g.*, overall amount of VAs owned by one or more subjects; detailed information on main movements of VAs traced back to the same subject or linked subjects in a specific timeframe; wallet/account statement in an editable format; and v) type and main features of VAs.

~~149.~~281. Since 2015, the Bank of Italy has warned consumers on the high risks of buying and/or holding VAs as well as supervised financial intermediaries about the possible risks associated with VAs. In particular, it issued a warning for consumers and a communication for supervised financial intermediaries (January 2015) as well as a new warning for consumers which recalled the one issued by the three European financial authorities—European Securities and Markets Authority (ESMA), the European Banking Authority (EBA), and the European Insurance and Occupational Pensions Authority (EIOPA) in March 2018. The Italian UIF, in order to enhance the engagement with the private sector, issued a Communication on January 30, 2015 about the anomalous use of crypto-assets, addressing particularly the financial institutions (*i.e.*, banks and payment institutions) as well as gambling operators, and underlining the necessity for these obliged entities to focus their attention on possible anomalous transactions, such as wire transfers, cash deposits and withdrawals, use of prepaid cards, associated with crypto-assets purchases or investments.

~~150.~~282. The UIF is progressing its analysis, focussing on new risks and emerging trends. An updated Communication was issued in 2019 to assist obliged entities in performing their tasks. In particular, the UIF updated its 2015 Communication on the anomalous use of crypto-assets by providing more details on recurring elements, operational methods, and behavioral risk profiles identified in STRs related to VAs. The Communication sets out specific instructions for filling in data in the pre-set STRs' format, particularly with reference to information about: VASPs, transactions, users/customers, and wallets/accounts.

~~151.~~283. In December 2016 and July 2018, the UIF published collections of sanitized cases of money laundering and terrorist financing that emerged in the course of financial analyses, including typologies connected to the anomalous use of VAs.

Norway

~~152.~~284. VASPs have been subject to the Norwegian AML Act and its obligations since October 15, 2018. The relevant provision of the AML regulation reads as follows:

Box 5. Section 1-3 Application of the Anti-Money Laundering Act to Virtual Currency

(1) Providers of exchange services between virtual currency and official currency are obliged entities within the meaning of the Anti-Money Laundering Act. This shall apply correspondingly to virtual currency custodianship services.

(2) By virtual currency is meant a digital expression of value, which is not issued by a central bank or a government authority, which is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but which is accepted as a means of exchange, and which can be transferred, stored or traded electronically.

(3) By virtual currency custodianship services is meant the custodianship of private cryptographic keys on behalf of customers, for purposes of transferring, storing or trading in virtual currency.

(4) The Financial Supervisory Authority may supervise compliance with the Anti-Money Laundering Act for the providers mentioned in paragraph 1. Providers as mentioned in paragraph 1, shall be registered with the Financial Supervisory Authority. The following information shall be registered on the provider:

a) name

b) type of enterprise and organisation number

c) business address

d) the service which is offered

e) name, residence address and personal identity number or D number on the

i) general manager or persons in a corresponding position

ii) members of the board of directors or persons in a corresponding position

iii) any other contact person

~~153.~~285. As of June 2019, six VAPSs have been registered, and more than 20 other VASPs have applied for registration, but have applications pending due to shortcomings in their AML policies and procedures. Three VA ATMs have been shut down in November 2018 after cease and desist orders from the FSA, and no new ATMs have been set up since. The FSA will commence inspections of the sector, but based on the registration applications in the second half of 2019, it is clear that the field of VASPs registered, and attempting to register, includes a range of actors with differences in size, competence, knowledge of AML rules, and professionalism.

Sweden

~~154.~~286. In Sweden, the Financial Supervisory Authority has considered bitcoin and ethereum as means of payment since 2013, meaning that professional exchange services are therefore subject to a licensing regime[51] and, following a successful application for a licence, AML/CFT supervision. The regulation is not an explicit AML/CFT regulation of VA exchange services as such (*i.e.,* they are not specifically mentioned in the law) but an implicit recognition that they should be regulated. Once an exchange service obtains a licence, all activities (*i.e.,* no matter the VA in question) are subject to AML/CFT regulation and supervision. Thematic supervision has been carried out. As a result, part of the sector has ceased its operations. VASPs have submitted STRs to the FIU, and feedback from operational authorities suggests that criminals are choosing to take their business to unregulated exchanges elsewhere.

Finland

~~155.~~287. The Act on Virtual Currency Providers (572/2019) came into force on May 1st 2019. VASPs are required to register (authorization) with the Finnish Financial Supervisory Authority (FIN-FSA).[52] Those who already provided services before legislation came into force, needed to be registered by November 1st 2019. New actors ~~have~~ had to be registered prior to starting their operations. The definition of VASPs includes exchanges (both fiat to VAs and between VAs as well as VAs and other goods such as gold), custodian wallet providers, and ~~ICOs~~issuers of virtual currency. The requirements for registration include basic fit and proper checks, requirements for handling customer funds, and simple rules regarding marketing (*i.e*., an obligation to give all relevant information and an obligation for truthful information). VASPs are obliged entities as defined in the AML Act (444/2017) and ~~are~~ were required to comply with AML/CFT obligations from December 1st 2019. VASP's AML/CFT risk assessment and their

51 It is not quite a comprehensive licensing regime in the prudential sense of the word, but for AML/CFT purposes it is, including fit and proper testing of owners and management and an assessment of whether the business will be conducted pursuant to AML/CFT regulation.

52 www.finanssivalvonta.fi/en/banks/fintech--financial-sector-innovations/virtuaalivaluutan-tarjoajat/

procedures and guidelines relating to AML/CFT are reviewed as part of the registration process.

156.288. FIN-FSA was given powers to issue regulations and guidance guidelines on certain parts of VASP activity. The FIN-FSA draft regulations and guidelines entered into force on July 1st 2019.[53] was published for consultation on May 21st. The draft contains regulationregulations contain regulation on holding and protecting client money and segregation of client money and own funds. Guidance Guidelines concern is given on compliance with AML/CFT regulationlegislation. The aim is to publish the regulation during summer.

157.289. Prior to the Act, the FIN-FSA has had been working with organizers of ICOs from the point of view of securities markets legislation and financial instruments. The aim hads been to identify when the VA wasis a financial instrument (*i.e.*, transferable security). These assessments are still required occasionally. In order to facilitate the assessment on the nature of the asset to be issued, For this purpose, the FIN-FSA has drafted a checklist that is used in all ICO-related enquiries. The checklist as well as frequently asked questions related to VAs are available at the FIN-FSA website.[54]

158.290. The FIN-FSA supervisory experience has shown that VASPs are now willing and keen on being regulated and trying to seek supervisors' endorsement for their activities. The challenge is to communicate to the general public that authorization does not equal endorsement. FIN-FSA has seen a total turn in VASPs attitude towards regulation. Some time ago they did not want to be regulated, but now they are seeking business models through which they could be regulated. VASPs have had challenges in opening bank accounts, which could partly explain the change in their attitude towards regulation.

Mexico

159.291. In Mexico, Federal Law *for the Prevention and Identification of Operations with Resources of Illegal Proceeds* was reformed in March 2018 to establish as a *Vulnerable Activity* the exchange of VAs made by entities other than Financial Technology Institutions and Credit Institutions.

160.292. Likewise, in March 2018, Mexico published the *Law to Regulate Financial Technology Institutions*, which indicates that Financial Technology Institutions may operate with VAs provided that they have the authorization of Bank of Mexico and operate with the VA that it determinates.

161.293. Subsequently, in September 2018, the standards that establish the measures and procedures in terms of AML/CFT related to VAs were published.

162.294. In March 2019, the Central Bank published the standards to define the internal operations that the Credit Institutions and the Financial Technology Institutions directly or indirectly pretend to carry out operations with VA.

163.295. The Central Bank said that VAs carry a significant ML/TF risk, due to the ease of transferring VA to different countries as well as the absence of homogeneous controls and prevention measures at the global level. However, it seeks to promote the use of technologies that could have a benefit, as long as these technologies are used internally between Financial Technology Institutions and Credit Institutions.

---

53 https://www.finanssivalvonta.fi/en/regulation/FIN-FSA-regulations/organisation-of-supervised-entities-operations/04_2019/.

54 www.finanssivalvonta.fi/en/banks/fintech--financial-sector-innovations/virtuaalivaluutan-tarjoajat/frequently-asked-questions-on-virtual-currencies-and-their-issuance-initial-coin-offering/

~~164.~~296. Finally, later in March 2019, the *Disposiciones de carácter general a que se refiere el Artículo 115 de la Ley de Instituciones Crédito* were reformed, establishing the measures and procedures that the credit institutions must follow to comply with the obligations regarding AML/CFT related to VAs.

Japan

~~165.~~297. Japan amended the *Payment Services Act and Act on Prevention of Transfer of Criminal Proceeds (*PTCP Act*)* in 2016 in response to the bankruptcy of a large VASP in 2014 and the 2015 FATF VC Guidance. Following the enactment of the laws in April 2017, the JFSA established a VASP monitoring team in August 2017, composed of AML/CFT and technology specialists.

~~166.~~298. As a part of its registration procedure, the JFSA assesses applicants' AML/CFT programs, with a focus on consistency between the applicants' risk assessment and their business plan, through document-based assessment and off-site or on-site interviews with them (as of March 2019, 19 VASPs are registered).

~~167.~~299. The JFSA imposes a periodical report-submission order on VASPs to seek quantitative and qualitative information on inherent risk and controls. The JFSA utilizes the collected information for its own risk assessment and monitoring of VASPs. The JFSA has conducted on-site inspections of 22 VASPs (including 13 then-deemed VASPs, *i.e.,* entities which were already in business before the enactment of the amended act, being allowed to operate on a tentative basis) and has imposed administrative dispositions (21 business improvement orders and six business termination orders and one refusal of registration) by March 2019.

~~168.~~300. The JFSA also closely co-operates with the Japan Virtual Currency Exchange Association (JVCEA), the self-regulatory body certified in October 2018, for prompt and flexible response to VASP-related issues. The JVCEA functions as an educational body and a monitoring body for the member VASPs. Compliance with self-regulatory AML/CFT rules and guidelines is prepared by the JVCEA. The JFSA, in consultation with the JVCEA, has conducted outreach, some of which was done in collaboration with other authorities, sharing information and ideas with VASPs that would contribute to improving their AML/CFT compliance.

~~169.~~301. In addition, the JFSA:

- Established the "*Study Group on the Virtual Currency Exchange Business*" in March 2018 to examine institutional responses to various issues related to the VASP business. In light of suggestions made on a report compiled by the Group, the JFSA, in March 2019, submitted to the Diet a bill to amend the acts. The amendment includes: the application of the Payment Services Act and PTCP Act to service providers who conduct custodian service of VAs; and the introduction of *ex ante* notification system concerning each change of a type of VA dealt in by VASPs taking into account the anonymity of VAs.
- Prepared and publicized red flag indicators of suspicious transactions, which are specific to VASPs, in April 2019. The indicators cover several transactions where anonymization technology was utilized.

United States

Comprehensive and Technology-Neutral Framework

~~170.~~302. The United States has a comprehensive and technology-neutral regulatory and supervisory framework in place for regulating and supervising "digital ~~financial~~ assets"[55] for AML/CFT that subjects covered providers and activities in this space to substantially the same regulation that providers of non-digital assets are subject to within the existing AML/CFT regulatory framework for ~~U.S. financial institutions~~FIs. The U.S. approach draws on the tools and authorities of various departments and agencies, including the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), the U.S. FIU and administrator of the primary U.S. AML law, the Bank Secrecy Act (BSA); U.S. Treasury's Office of Foreign Assets Control (OFAC); the Internal Revenue Service (IRS); the U.S. Securities and Exchange Commission (SEC); the U.S. Commodity Futures Trading Commission (CFTC); and other departments and agencies. FinCEN, the IRS, the SEC, and the CFTC in particular have regulatory, supervisory, and enforcement authorities to oversee certain digital asset activities that involve money transmission; securities, commodities, or derivatives; or that have tax implications, and they have authority to mitigate the misuse of digital assets for illicit financial transactions or tax avoidance.

~~171.~~303. Where a person (a term defined in U.S. regulation that goes beyond natural and legal persons) engages in certain financial activities involving digital assets, AML/CFT and other obligations apply. Depending on the activity, the person or institution is subject to the supervisory authority of FinCEN, the SEC, and/or the CFTC to regulate the person as a money transmitter, national securities exchange, broker-dealer, investment adviser, investment company, transfer agent, designated contract market, swap execution facility, derivatives clearing organization, futures commission merchant, commodity pool operator, commodity trading advisor, swap dealer, major swap participant, retail foreign exchange dealer, or introducing broker.

~~172.~~304. If the person falls under the regulatory definition of a "bank," FinCEN and the U.S. federal banking agencies—the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, and National Credit Union Administration—have authority, sometimes concurrent with that of the state banking regulators, to regulate and supervise persons when they engage in financial activity involving digital assets. Moreover, existing general tax principles apply to transactions involving digital assets in the United States because the IRS classifies them as property.

Box 6. Case Study: U.S. Regulation and Supervision (Including Licensing and Registration) of Digital Asset-Related Providers

[55] ~~From a U.S. perspective, the term "digital financial assets" (or "digital assets") is a comprehensive term that refers to a range of activities in the digital financial services ecosystem, including financial activities involving digital currencies—both national digital currencies and digital currencies that are not issued or guaranteed by a national government, such as digital forms of convertible virtual currencies like bitcoin—as well as digital securities, digital commodities, or digital derivatives thereof.~~From a U.S. perspective, the term "digital assets" is a comprehensive term that refers to a range of assets in the digital financial services ecosystem, including digital currencies—both national digital currencies and digital currencies that are not issued or guaranteed by a national government, such as convertible virtual currencies like bitcoin—as well as digital assets that are securities, commodities, or derivatives thereof.

Money Transmission. At the federal level, FinCEN regulates as money transmitters any person engaged in the business of accepting and transmitting value, whether physical or digital, that substitutes for currency (including convertible virtual currency, whether virtual-to-virtual, virtual-to-fiat, or virtual-to-other value) from one person to another person or location by any means. Under the BSA, money transmitters must register with FinCEN as money services businesses and institute AML programs, recordkeeping, and reporting measures, including filing suspicious activity reports. The AML requirements apply equally to domestic and foreign-located money transmitters, even if the foreign-located entity does not have a physical presence in the United States and regardless of where it is incorporated or headquartered, as long as it does business in whole or substantial part in the United States. Since 2014, the IRS and FinCEN have conducted examinations of various digital asset-related providers, including administrators, some of the largest exchangers by volume, ~~individual peer-to-peer~~ exchangers allowing exchanges between individual users, foreign-located exchangers, digital asset/crypto-precious metal dealers, kiosk companies, and numerous trading platforms as well as registered and unregistered financial institutions. Applicable state laws also require relevant covered entities to obtain state money transmitter licenses in most states in which they operate, regardless of their jurisdiction of incorporation or the physical location of their head office. Money transmitters also may be subject to other regulatory requirements, including safety, soundness, and capital reserve requirements, depending on the U.S. state in which they are located or do business and whether or not their operations make them subject to the rules of other U.S. regulatory bodies.

Securities Activity. To the extent a digital asset is a security in the United States, the SEC has regulatory and enforcement authority that extends to the offer, sale, and trading of, and other financial services and conduct relating to, those digital assets. Platforms on which digital assets that are securities are traded in the secondary market generally must register as national securities exchanges or operate pursuant to an exemption from registration, such as the exemption under SEC requirements for alternative trading systems (*i.e.*, SEC Regulation ATS), and report information about their operations and trading to the SEC. Even if the securities exchange, broker-dealer, investment adviser or other ~~similar~~ securities-related entity is a foreign-located person and does not have a physical presence in the United States, the person may be subject to SEC regulations and jurisdiction when they offer, sell, or conduct activities relating to ~~issue~~ securities (including, digital assets that are securities~~potentially, certain ICO tokens~~) to U.S. persons ~~or investors~~ or otherwise affect the U.S. securities markets. Additional state licensing obligations may apply depending on the activity in which an entity is engaged and on the state in which the activity is conducted. Certain trading in digital assets, including trading on platforms, may still qualify as money transmission under the BSA and state laws or regulations, as discussed above. If the digital asset is a security, it is subject to SEC jurisdiction and any derivatives on the security ~~is~~ are subject to SEC jurisdiction.

Commodities and Derivatives Activity. In the United States, a digital asset~~s~~ may also be considered as ~~qualify as~~ commodities ~~or derivatives thereof, even if not a security, in which case persons dealing in such digital assets are~~ subject to CFTC jurisdiction.[56]

[56] The CFTC has determined that "virtual currency" is a commodity as that term is defined by CEA section 1a(9). *In re Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, CFTC Docket No. 15–29, 2015 WL 5535736, [Current Transfer Binder] Comm. Fut. L. Rep. (CCH) paragraph 33,538 (CFTC Sept. 17, 2015) (consent order); In re TeraExchange LLC, CFTC Docket No. 15–33, 2015 WL 5658082, [Current Transfer Binder] Comm. Fut. L. Rep. (CCH) paragraph 33,546 (CFTC Sept. 24, 2015) (consent order).*

With certain exceptions, the CFTC has full regulatory authority and exclusive jurisdiction over all commodity futures, options, and all other derivatives that fall within the definition of a swap, including derivatives on digital assets.[57] ~~The CFTC has full regulatory authority over derivatives on digital assets that are not securities (*e.g.*, futures contracts).~~ The CFTC exercises anti-fraud and anti-manipulation regulatory authority over the sale of such assets and requires registration in connection with trading in futures and options thereon or certain other derivatives on such for commodities. Pursuant to the Commodity Exchange Act and related r~~R~~egulations, the CFTC has broad authority to take action against any person or entity located inside or outside the United States that is associated with or engaged in fraud or manipulative activity (*e.g.*, U.S. CFTC *v.* Blue Bit Banc).

Generally, a natural or legal person that transacts in securities, commodities or derivatives is subject to additional oversight by a self-regulatory organization. Securities activities require registration with the Financial Industry Regulatory Authority (FINRA), and commodities and derivatives activities require registration with the National Futures Association (NFA). Depending on its activities, a natural or legal person may also require dual registration with FINRA and the NFA, both of which have statutory obligations under U.S. federal securities and commodities laws. Additionally, similar to money transmitter licenses, a natural or legal person must be licensed with each state regulator~~y~~ for states in which they do business.

Certain registrants of the SEC and CFTC also have BSA obligations, including establishing AML programs, reporting suspicious activity to FinCEN, identifying and verifying customer identity, and applying enhanced due diligence for certain accounts involving foreign persons. The relevant regulatory and supervisory bodies also monitor digital asset activities and examine registrants for compliance with their regulatory obligations, including (for certain registrants) AML/CFT obligations under the BSA.

U.S. Law Enforcement, Sanctions, and Other Enforcement Capabilities

~~173.~~305. U.S. law enforcement uses financial intelligence information from FinCEN to conduct investigations involving digital assets. Such information—which is sourced from the reporting and analysis that FinCEN collects and disseminates to competent U.S. law enforcement authorities—has been useful in developing evidence of criminal activity and identifying individuals who may be involved in ML or TF activities. FinCEN has access to a wide range of financial, administrative, and law enforcement information. The information at FinCEN's disposal includes two key pieces of information that can be instrumental in detecting suspected ML or TF involving digital assets: (i) suspicious activity reports (or ~~STRs~~SARs) filed by traditional reporting financial institutions, such as banks or broker-dealers in securities for example, that have transmitted fiat currency for conversion or exchange into a digital asset at a digital asset exchanger or related business or that have received fiat currency from a digital asset exchanger or related business after being converted or exchanged from a digital asset; and (ii) ~~suspicious activity reports~~SARs filed by digital asset providers that, often operating as money transmitters, receive funds and convert them into a digital asset or allow for the storage and/or trading and exchange of digital assets. FinCEN also collects other information, such as foreign bank account, currency and monetary instrument, and currency transaction reports—all of which could

[57] U.S.C. 2(a)(1)(A). The CFTC shares its swap jurisdiction in certain aspects with the SEC. *See* 7 U.S.C. 2(a)(1)(C).

contain investigative leads and evidence necessary to deter and prosecute criminal activity associated with digital assets.

~~174.~~306. U.S. departments and agencies have taken strong civil and criminal enforcement actions in both administrative proceedings and federal court to combat illicit activity relating to digital assets, such as by seeking various forms of relief, including cease and desist orders, injunctions, disgorgement with prejudgment interest, and civil money penalties for wilful violations and imposing criminal sentences involving forfeiture and imprisonment.[58] U.S. regulators and supervisors engage extensively with one another, state regulators, the U.S. Department of Justice (DOJ), and other law enforcement agencies to support investigative and prosecutorial efforts in the digital assets space.

~~175.~~307. A variety of criminal and civil authorities, policy tools, and legal processes exist to assist U.S. government agencies in identifying illicit digital asset-related activity, attributing transactions to a specific individual or organization, mitigating threats, and performing analysis relating to their respective regulatory or criminal investigative functions. For such investigations and prosecutions, DOJ relies on a range of statutory criminal and civil authorities, including federal laws governing money laundering, money services businesses registration, financial institution recordkeeping and reporting requirements, fraud, tax evasion, the sale of controlled substances and other illegal items and services, computer crimes, and terrorist financing. The United States has charged and prosecuted individuals operating as peer-to-peer exchangers for violating the BSA or for money laundering as well as foreign-located persons and organizations who violate U.S. law, among other prosecutions relating to digital assets.

~~176.~~308. Similar to FinCEN, SEC, and CFTC authorities, DOJ has broad authority to prosecute digital asset providers and individuals who violate U.S. law, even though they may not be physically located inside the United States. Where digital asset transactions touch financial, data storage, or other computer systems within the United States, for example, the DOJ has jurisdiction to prosecute persons directing or conducting those transactions. The United States also has jurisdiction to prosecute foreign-located persons who use digital assets to import illegal products or contraband into the United States or who use U.S.-located digital asset businesses or providers or financial institutions for money laundering purposes. In addition, foreign-located persons who provide illicit services to, defraud, or steal from U.S. residents may be prosecuted for violations of U.S. law.

~~177.~~ OFAC, typically in consultation with other agencies, administers U.S. financial sanctions and associated licensing, regulations, and penalties, all of which relate to digital assets as well as most other types of assets. OFAC has made clear that U.S. sanctions compliance obligations are the same, regardless of whether a transaction is denominated in digital ~~currency~~ assets (whether national digital currency or non-national digital currency such as convertible virtual currency like bitcoin) or traditional fiat currency, and U.S. persons and persons otherwise subject to OFAC jurisdiction are responsible for ensuring they do not engage in unauthorized transactions prohibited by OFAC sanctions. OFAC's December 2020 enforcement action and associated fine for failures related to VA services provides further confirmation of this.[59]

---

58 *Select examples of U.S. enforcement, investigative, and/or sanctions actions include:* 2015 civil money penalty against Ripple Labs, Inc.; 2016 Operation Dark Gold; 2017 civil money penalties against BTC-e and concurrent indictment of Alexander Vinnik; 2017 TF case, *U.S. v. Zoobia Shahnaz*; 2018 sentencing of unlicensed bitcoin trader; and 2019 identification of digital currency addresses associated with OFAC SamSam designation.

59 https://home.treasury.gov/system/files/126/20201230_bitgo.pdf.

309.

International Co-operation is Key

~~178.~~310. The inherently global nature of the digital asset ecosystem makes digital asset activities particularly well suited for carrying out and facilitating crimes that are transnational in nature. Customers and services can transact and operate with little regard to national borders, creating jurisdictional hurdles. Effectively countering criminal activity involving digital assets requires close international partnerships.

~~179.~~311. U.S. departments and agencies, particularly U.S. law enforcement, work closely with foreign partners in conducting investigations, making arrests, and seizing criminal assets in cases involving digital asset activity. The United States has encouraged these partnerships to support multi-jurisdictional investigations and prosecutions, particularly those involving foreign-located persons, digital asset providers, and transnational criminal organizations. Mutual legal assistance requests remain a key mechanism for enhancing co-operation. Because illicit actors can quickly destroy, dissipate, or conceal digital assets and related evidence, the United States has developed policies for obtaining evidence and restraining assets located abroad, recognizing that digital assets and the associated transactional data and evidence may be stored or located via technological means and processes not contemplated by current legal methods and treaties.

Section VI – PRINCIPLES OF INFORMATION-SHARING AND CO-OPERATION AMONGST VASP SUPERVISORS

312. The FATF Recommendations encourage providing the fullest range of international co-operation. INR. 15 states that countries should rapidly, constructively, and effectively provide the widest possible range of international co-operation in relation to money laundering, predicate offences, and terrorist financing relating to VAs, on the basis set out in Recommendations 37 to 40. In particular, supervisors of VASPs should exchange information promptly and constructively with their foreign counterparts, regardless of the supervisors' nature or status and differences in the nomenclature or status of VASPs. Further information on the application of Recommendations 37 to 40 to VAs is set out in Section III above.

Objectives

313. Each country must designate at least one competent authority as their supervisor of VASPs for AML/CFT purposes. Other than specifying that the competent authority cannot be a self-regulatory body, the FATF Standards do not specify who the competent authority should be. Countries have designated a range of different authorities as VASP supervisors, including financial services supervisors, central banks, securities regulators, tax authorities, FIUs and specialist VASP supervisors. Some countries have one single supervisor while others have multiple supervisors. Some countries treat VASPs as a clearly-identifiable, specific category of business, while others consider VASPs to be a sub-set of pre-existing business categories (e.g. as money service businesses).

314. The FATF Standards make clear that supervisors should exchange information promptly and constructively with their foreign counterparts, regardless of the supervisors' nature or status and differences in the nomenclature or status of VASPs. Given the pseudonymous, fast-paced, cross-border nature of VAs, international co-operation is all the more critical between VASP supervisors. To facilitate co-operation between counterparts

and exchange relevant information, the FATF has developed **Principles of Information-Sharing and Co-operation** between VASP Supervisors. These principles are intended to:

a) provide a common understanding of the type of supervisory information and other background knowledge that will be useful for authorities to share with each other and when to share such information;

b) outline possible triggers for proactive information sharing/requests, for example when a cybersecurity incident has taken place that has potential AML/CFT impact on other jurisdictions or where a foreign-based VASP is potentially conducting unregulated VASP activity in a jurisdiction;

c) set out possible methods of sharing and types of supervisory assistance/feedback that could be adopted in certain circumstances (in line with confidentiality provisions);

d) set out possible roles and expectations where multiple AML/CFT supervisors are working together on a specific case or issue;

e) suggest possible guidelines for jurisdictions, when dealing with issues with VASPs in jurisdictions that do not have regulatory frameworks in place, or when seeking to facilitate supervisory co-operation for multijurisdictional VASPs; and

f) set out best practice in relation to the types of information countries should maintain on licensed/registered VASPs, as part of their respective directories or websites.

315. These Principles are **non-binding** on supervisors. They are intended as guidance for supervisors. Supervisors are not obliged to adopt and implement these Principles, nor are Supervisors obliged to share information or render co-operation unless it is consistent with their domestic frameworks (which could condition co-operation and exchange of information on the adoption of legal arrangements such as Memorandums of Understanding) and does not contradict the obligations arising from R. 37-40.

316. These Principles are, however, applicable to all countries, whether they permit or prohibit VASPs. Countries that prohibit VASPs must have a legal basis for permitting their relevant competent authorities to exchange information on issues related to virtual assets and VASPs. This competent authority may not be a supervisor, but may be, for example, a law enforcement agency.

Principles of Information-Sharing and Co-operation

317. International co-operation between Supervisors should be encouraged and based upon a foundation of mutual trust. Information-sharing arrangements must recognize and allow room for case-by-case solutions to specific problems.

Identification of Supervisors and VASPs

1. Countries must clearly identify their Supervisor(s) of VASPs for AML/CFT purposes. Where a country has multiple Supervisors, the country should clearly identify the scope of each Supervisors' regulatory remit.

2. Supervisors should have a clear mechanism by which to receive inquiries relating to VASPs. For example, this could be a specific email address for VASP-related inquiries.

3. To facilitate timely co-operation, Supervisors should ensure that information on licensed or registered VASPs under their purview is readily accessible by foreign authorities. This could be done, for example, through the publication of public

registers of obliged entities, or the maintenance of a licensed/registered entities database that can be queried through secure information exchange.

Information exchange

4. Supervisors should exchange relevant information on VASPs with foreign Supervisors, regardless of their status. To this end, Supervisors should have an adequate legal basis for providing co-operation on money laundering, associated predicate offences and the financing of terrorism.

5. There are a number of methods by which supervisory information could be exchanged. Most typically, information could be exchanged bilaterally, upon request from one Supervisor to another. Where VASPs are multilateral in nature, supervisors may also decide to share information multilaterally, with all other regulators of the VASP. Lastly, less sensitive supervisory information could be shared as necessary, at supervisory colleges organized by lead supervisors of multilateral VASPs. Given the cross-border nature of VASPs, the development of supervisory colleges for larger multilateral VASPs could serve to enhance overall AML/CFT supervision of these entities.

6. The types of information exchanged between supervisors would depend on a range of factors such as the trigger(s) for the exchange of information, statutory and/or blockchain data obtained by the Supervisor rendering assistance, and countries' domestic legal frameworks. Where available and legally permitted, supervisors should provide where relevant, information such as a VASP's regulatory status, details of its shareholders and directors, transaction-related data and customer information (which could have been obtained from supervisory activities, statutory returns, and blockchain surveillance and analytical tools). Supervisors should also consider exercising its supervisory powers to obtain further information from the VASP, where necessary.

7. A Supervisor requesting information should disclose, to the Supervisor that will process the request, the reason for the request, and to the extent possible the purpose for which the information will be used, and provide enough information to enable the Supervisor receiving the request to provide information lawfully.

8. Supervisors should acknowledge receipt of requests, respond to requests for information, and provide interim partial or negative responses in a timely manner.

9. Supervisors should not prohibit or place unreasonable or unduly restrictive conditions on exchanging information or providing assistance. In particular, Supervisors should not refuse a request for assistance on the grounds that:

   a. laws require FIs, DNFBPs or VASPs (except where the relevant information that is sought is held under circumstances where legal privilege or legal professional secrecy applies) to maintain secrecy or confidentiality;

   b. there is an inquiry, investigation or proceeding underway in the country receiving the request, unless the assistance would impede that inquiry, investigation or proceeding; and/or

   c. the nature or status of the requesting counterpart authority is different to its foreign Supervisor.

10. Information received, processed, held or disseminated by requesting Supervisors must be securely protected, exchanged and used only in accordance with agreed procedures, policies and applicable laws and regulations.

11. Exchanged information should be used only for the purpose for which the information was sought or provided. Any dissemination of the information to other authorities or third parties, or any use of this information for administrative, investigative, prosecutorial or judicial purposes, beyond those originally approved, should be subject to prior authorization by the requested Supervisor. At a minimum, the requesting financial supervisor should promptly inform the requested Supervisor of its legal obligation to disclose or report the information to a third party.

12. Supervisors should be proactive in raising material issues and concerns with other Supervisors and should respond in a timely and satisfactory manner when such issues and concerns are raised with them.

13. Supervisors should consider proactively sharing information or requesting information as necessary to carry out their supervisory functions. Possible triggers for such a request include:

    a. when a cybersecurity incident has taken place in a local VASP that has potential AML/CFT impact on other jurisdictions;

    b. where a foreign-based VASP is potentially conducting unregulated VASP activity in a jurisdiction; and

    c. where a local VASP is strongly suspected to be facilitating illicit ML/TF activity, and has substantial operations based in foreign jurisdictions.

14. Upon request and whenever possible, Supervisors should provide feedback to their foreign counterparts on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided.

15. Supervisors should communicate emerging issues and developments of a material and potentially adverse nature, including supervisory actions, with other relevant Supervisors of the VASP in a timely manner.

16. Supervisors should share, with other relevant Supervisors of the VASP, information affecting the regulated entity for which the latter have responsibility, including supervisory actions, except in unusual circumstances when supervisory considerations dictate otherwise.

Co-operation

17. In some instances, a primary Supervisor could be identified if the VASP has significant proportion of its business operations in a jurisdiction. While supervisors should work together to identify a primary Supervisor who could act as a focal point through which to coordinate information sharing and co-operation, such identification is not mandatory and does not absolve other Supervisors of the responsibility to supervise the VASP in their respective jurisdictions.

18. Supervisors should use the most efficient means to co-operate. If bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), are needed, these should be negotiated and signed in a timely way with the widest possible range of foreign Supervisors in the context of international co-operation to counter money laundering, associated predicate offences and terrorist financing.

19. Supervisors should be able to conduct queries on behalf of foreign Supervisors, and exchange with these foreign Supervisors all information that they would be able to obtain if such queries were carried out domestically.

20. When requesting co-operation, Supervisors should make their best efforts to provide complete, factual and, as appropriate, legal information including the description of the case in concern. This includes indicating any need for urgency, to enable timely and efficient execution of the requests for co-operation.

Annex A. Recommendation 15 and its Interpretive Note and FATF Definitions

Recommendation 15 – New Technologies

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

Interpretative Note to Recommendation 15

1. For the purposes of applying the FATF Recommendations, countries should consider virtual assets as "property," "proceeds," "funds," "funds or other assets," or other "corresponding value." Countries should apply the relevant measures under the FATF Recommendations to virtual assets and virtual asset service providers (VASPs).

2. In accordance with Recommendation 1, countries should identify, assess, and understand the money laundering and terrorist financing risks emerging from virtual asset activities and the activities or operations of VASPs. Based on that assessment, countries should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. Countries should require VASPs to identify, assess, and take effective action to mitigate their money laundering and terrorist financing risks.

3. VASPs should be required to be licensed or registered. At a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created.[1] In cases where the VASP is a natural person, they should be required to be licensed or registered in the jurisdiction where their place of business is located. Jurisdictions may also require VASPs that offer products and/or services to customers in, or conduct operations from, their jurisdiction to be licensed or registered in this jurisdiction. Competent authorities should take the necessary legal or regulatory 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. Countries should take action to identify natural or legal persons that carry out VASP activities without the requisite license or registration, and apply appropriate sanctions.

4. 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.

5. Countries should ensure that VASPs are subject to adequate regulation and supervision or monitoring for AML/CFT and are effectively implementing the relevant FATF Recommendations, to mitigate money laundering and terrorist financing risks

emerging from virtual assets. VASPs should be subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements. VASPs should be supervised or monitored by a competent authority (not a SRB), which should conduct risk-based supervision or monitoring. Supervisors should have adequate powers to supervise or monitor and ensure compliance by VASPs with requirements to combat money laundering and terrorist financing including the authority to conduct inspections, compel the production of information, and impose sanctions. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the VASP's license or registration, where applicable.

6. Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with VASPs that fail to comply with AML/CFT requirements, in line with Recommendation 35. Sanctions should be applicable not only to VASPs, but also to their directors and senior management.

7. With respect to preventive measures, the requirements set out in Recommendations 10 to 21 apply to VASPs, subject to the following qualifications:

8. (a) R.10 – The occasional transactions designated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000.

9. *(b) R.16* – Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information[2] on virtual asset transfers, submit[3] the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities. Countries should ensure that beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers, and make it available on request to appropriate authorities. Other requirements of R.16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the same basis as set out in R.16. The same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer.

10. 8. Countries should rapidly, constructively, and effectively provide the widest possible range of international co-operation in relation to money laundering, predicate offences, and terrorist financing relating to virtual assets, on the basis set out in Recommendations 37 to 40. In particular, supervisors of VASPs should exchange information promptly and constructively with their foreign counterparts, regardless of the supervisors' nature or status and differences in the nomenclature or status of VASPs.

[1] References to creating a legal person include incorporation of companies or any other mechanism that is used.

[2] As defined in INR. 16, paragraph 6, or the equivalent information in a virtual asset context.

[3] The information can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to virtual asset transfers.

FATF Glossary

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

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) transfer[1] 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.

Annex B. Summary of changes made to this Guidance

Note: This section will be added once the changes to the document are finalised.