FATF

Appendix I

GUIDANCE FOR A RISK-BASED APPROACH

VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS

JUNE 2019

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

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

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

Citing reference:

FATF (2019), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,* FATF, Paris,
www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

Photocredits coverphoto ©Getty Images

Table of contents

ACRONYMS

AEC	Anonymity-Enhanced Cryptocurrency
AML	Anti-Money Laundering
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
DNFBP	Designated Non-Financial Business and Profession
ICO	Initial Coin Offering
ML	Money Laundering
MSB	Money Services Business
MVTS	Money or Value Transfer Service
OTC	Over-the-Counter
P2P	Peer-to-Peer
RBA	Risk-Based Approach
TF	Terrorist Financing
VA	Virtual Asset
VASP	Virtual Asset Service Provider

EXECUTIVE SUMMARY

In October 2018, the 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, licenced 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 the present Guidance[1] on the application of the RBA to VAs and VASPs In June 2019. It is intended to 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 ML/TF risks associated with their activities and take appropriate mitigating measures to address them. 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 that would 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 brokerdealers, 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 are still relevant and applicable. VASPs therefore have the same full set of obligations as financial institutions or DNFBPs.

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 valuebased terms in the FATF Recommendations (*e.g.*, "property," "proceeds," "funds," "funds or

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

other assets," and other "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 chose 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 countries which have chosen to prohibit VA and VA activities at national level.

Regarding VASP supervision, the Guidance makes clear that only competent authorities 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 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). 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.

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.

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 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.

Purpose of the Guidance

8. 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. 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 riskbased 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. 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. 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. While the FATF notes that some governments are considering a range of regulatory responses to VAs and to the regulation of VASPs, many jurisdictions do not yet have 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 may come into play and shape the regulatory response to the VASP sector in individual jurisdictions.

Scope of the Guidance

13. 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 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.

14. Further, the Guidance focuses on VAs that are convertible for 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 protection, prudential safety and soundness, tax, anti-fraud or anti-market manipulation issues, network IT security standards, or financial stability concerns).

15. 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.

16. 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,[2] 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 competent authorities and VASPs should consider in devising appropriate solutions.

17. 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.

18. Other stakeholders, including FIs and other obliged entities that provide banking services to VASPs or to customers involved in VA activities or that engage in VASP activities themselves should also consider the aforementioned factors. 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 a proper risk assessment.

19. 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 of their laws and regulations. The Guidance seeks to support ends-based or objectives-based implementation of

[2] 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 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 are 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 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*. 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.

20. 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

21. 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.

22. Annexes 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, the updated text of Recommendation 15 and its Interpretive Note, and the "virtual asset" and "virtual asset service provider" definitions within the FATF Glossary.

SECTION II – SCOPE OF FATF STANDARDS

23. 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.

24. It should be underscored that when VASPs engage in traditional fiat-only activities or fiat-tofiat 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

25. The FATF Recommendations do not predetermine any sector as higher risk. The standards identify sectors that may be vulnerable to ML and TF; however the overall risk should be determined 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, 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 termination or restriction of business relationships with a particular sector (*e.g.*, FI relationships with VASPs, where relevant) to avoid, rather than manage, risk in line with the FATF's risk-based approach.

26. The FATF has assessed that ML/TF risks exist in relation to VAs, VA financial activities or operations, and VASPs. Accordingly, 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.

27. 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; and type(s) of VA exchanged, among other factors.

28. 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 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 in VA financial activities or operations may indicate higher ML/TF risks. 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 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.

29. 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 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.

30. 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. 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.

31. In addition to consulting the previous FATF works on this subject,[3] countries and VASPs should consider the following 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:

    a) 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-tovirtual transactions;

    b) The risks associated with centralised and decentralised VASP business models;

    c) 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;

    d) The specific business model of the VASP and whether that business model introduces or exacerbates specific risks;

    e) 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);

    f) Exposure to Internet Protocol (IP) anonymizers such as The Onion Router

[3] 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.

(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;

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

h) 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);

i) 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

j) 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).

32. Some countries may decide to prohibit VA activities or VASPs, 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 protection, safety and soundness, 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 (see sub-section 3.1.1.).

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

33. The FATF Recommendations require all jurisdictions to impose specified AML/CFT requirements on FIs and DNFBPs 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[4] 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.

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

35. 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.

36. 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.

37. 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.[5] 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.

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

[5] 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.

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.

38. 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,[6] 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;[7] 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.

39. 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-toindividual 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 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.

40. 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

[6] 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.

[7] 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. EtherDelta (U.S. Securities and Commission case, November 2018) 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-topeer 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.)

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.[8] 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.

41. 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.

42. 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.[9] 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.

43. 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.

44. 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").

45. 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 competent authorities in jurisdictions should therefore strive to

[8] 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 www.sec.gov/litigation/investreport/3481207.pdf.

[9] 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)*

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.

46. 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.

47. 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[10]—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.

48. 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.

49. 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 technologyneutral. Rather, the framing of the Recommendations, including Recommendation

[10] 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.

15, is activity-based and focused on functions in order to provide jurisdictions with sufficient flexibility.

50. 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. 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.

51. 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.

52. 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).

53. 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).

54. VASPs are subject to the relevant FATF measures that are similarly applicable to other entities subject to AML/CFT regulation under the FATF Recommendations, regardless of what a jurisdiction may term such providers, based on the types of activities in which VASPs engage. Further, as described in INR. 15, the measures applicable to "property," "proceeds," "funds," "funds or assets," and other "corresponding value" under the FATF Recommendations also apply to VAs (*e.g.*, Recommendations 3 – 8, 30, 33, 35, and 38).

SECTION III – APPLICATION OF FATF STANDARDS TO COUNTRIES AND COMPETENT AUTHORITIES

55. 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 are still relevant and applicable.

56. 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.

57. 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

58. **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, and the activities or operations of VASPs, the distinction between centralized and decentralized VAs, 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 customer identification and verification, VAs and VASPs in general may be regarded as higher ML/TF risks that may potentially require the application of enhanced due diligence measures, where appropriate.

59. 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.

60. 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.

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

62. 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.

63. A jurisdiction has the discretion to prohibit VA activities or VASPs, 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 protection, safety and soundness, or monetary policy). 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 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. 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.

64. **Recommendation 2** requires national co-operation and co-ordination with respect to AML/CFT 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 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 crossborder 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 cooperation 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

65. 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.

66. **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.

67. **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.

68. 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.

69. **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).

70. **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.

71. **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.

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

73. **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).

74. **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.

75. **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.

76. **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

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

78. 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[11] 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.

79. 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 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 a potential factor for consideration, the location of the server of the business.

80. VASPs that are licensed or registered should be required to meet appropriate licensing and registration criteria set by relevant authorities. Authorities should impose such conditions on licenced 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.

81. 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.

[11] See footnote 40 in INR. 24.

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.

82. 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. Such measures should include requiring VASPs to seek authorities' prior approval for substantive changes in shareholders, business operations, and structures.

83. 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 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 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 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.

84. In order to identify persons operating without a license and/or registration, countries should consider the range of tools and resources they may have for investigating the presence of an unlicensed or unregistered VASP. For example, countries should consider web-scraping and open-source information to identify online advertising or possible solicitations for business by an unregistered or unlicensed entity; information from industry circles (including by establishing channels for receiving public feedback) regarding the presence of certain businesses that may be unlicensed or unregistered; FIU or other information from reporting institutions, such as STRs or bank-provided investigative leads that may reveal the presence of an unlicensed or unregistered natural or legal person VASP; non-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; as well as other investigative tools or capabilities.

85. 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. Countries should have in place relevant channels for sharing information as appropriate to support the identification and sanctioning of unlicensed or unregistered VASPs.

Supervision or Monitoring

86. **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, 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.

87. 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 cooperation 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.[12]

88. 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.[13]

Preventive Measures

89. 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 following subsection 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.

90. **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.

91. **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

[12] 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.

[13] 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.

understanding the purpose and intended nature of the business relationship, where relevant, and obtaining further information in higher risk situations.

92. 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).[14]

93. 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.

94. 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 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.

95. 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" 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 or performed by VASPs (as well as other obliged entities, such as banks that engage in VA activities), including "occasional transactions" 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.

96. 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 (see INR. 10, paragraph 15(b)).

97. 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:

[14] 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.

a) Countries or geographic areas identified by credible sources[15] 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;

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, and for which financial institutions should give special attention to business relationships and transactions.

98. 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.

99. In these and other cases, the enhanced due diligence (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; and

c) 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.16

100. Countries also should consider the enhanced CDD 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. Additionally, countries should consider the measures required for FIs that engage in fiat-denominated activity that is non-face-to-face (such as mobile

15 "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.

[16] 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.

services) or that is comparable to VA transactions in assessing their risks and developing mitigating controls accordingly.

101. 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.

102. **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.

103. 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 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.

104. **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)[15] or 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.

105. **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

[15] "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).

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*).

106. To the extent that relationships in the VASP sector currently have or may in the future[16] 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.

107. **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 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).

108. **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).

109. 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).

110. 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

[16] 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.

cannot manage and mitigate the risks posed by engaging in such activities, then the VASP should not be permitted to engage in such activities.

111. **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.

112. 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.

113. 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.

114. 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[17] 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

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

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.

115. 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.)

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

117. 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.

118. 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).

119. 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 distributed ledger platform itself. Submitting information to the beneficiary VASP could be an entirely distinct process from that of the blockchain or other distributed ledger 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).

120. **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.

121. 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.

122. **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.

123. **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.

124. **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).

125. 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).

126. 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. [18] 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.

127. **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

128. **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

129. **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.

130. 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.

[18] 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.

131. **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.

132. **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.

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

134. **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

135. **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.

136. 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.

137. 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.

138. 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 subsections 3.1.4 and 3.18 above).

139. 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 information on relevant STRs with their counterparts in a timely manner, especially in relation to crossborder 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.

DNFBPs that Engage in or Provide Covered VA Activities

140. 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.

141. 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.

Risk-Based Approach to Supervision or Monitoring of VASPs

Understanding the ML/TF Risks

142. 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.

143. 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 associated with individual VASPs and specific VA products, services, or activities.

144. 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.

145. 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.

146. 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.

147. 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.

148. 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, [19] 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.

149. 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.

150. 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

151. 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 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 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). 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

[19] 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.

the categorisation of individual VASPs within the sector based on their customer base, the countries they deal with, and their applicable AML/CFT controls.

152. 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.

153. 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 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*: 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.

154. 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

155. 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.

156. Supervisors should ensure that their staff is 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.

157. 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.

158. 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 coordinate 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.

Guidance

159. 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.

160. 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.

161. 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.

162. 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

163. 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.

164. 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.

165. 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

166. 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.

167. 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.

168. 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.

169. 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.

SECTION IV – APPLICATION OF FATF STANDARDS TO VASPS AND OTHER OBLIGED ENTITIES THAT ENGAGE IN OR PROVIDE COVERED VA ACTIVITIES

170. 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.

171. 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.

172. 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.

173. **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.

174. 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.

175. 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).

176. 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.

177. 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; geolocation data; device identifiers; VA wallet addresses; and transaction hashes.

178. 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.[20]

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

179. 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 describe 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 VASPs' 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.

180. 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 determined whether additional mitigating or preventive actions are warranted if there is a positive hit.

181. 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)

182. 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.

183. 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.

184. VASPs and other obliged entities should adjust the extent and depth of their monitoring in line with their institutional risk assessment and individual customer risk profiles. 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.

185. 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.

186. **Recommendation 12.** For domestic PEPs[21] and international organisation PEPs,[22] 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.[23]

187. **Recommendation 16.** As noted in Section III, providers in this space must comply with the requirements of Recommendation 16, including the obligation to obtain, hold, and transmit 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.

188. 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

[21] "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).

[22] "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).

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

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.

189. 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.

190. 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 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.

191. **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.

192. 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.

193. **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-tovirtual, 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.

194. 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.

195. 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.

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

196. 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

197. 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.

198. 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.

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

200. 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.

201. 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.

202. 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.

203. 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.

204. 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

205. 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:

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

206. 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

207. 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[24] 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

208. 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 (FINFSA).[25] Those who already provided services before legislation came into force, need to be registered by November 1st 2019. New actors have 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. 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 required to comply with AML/CFT obligations from December 1st 2019. VASP's AML/CFT risk assessment and their procedures and guidelines relating to AML/CFT are reviewed as part of the registration process.

209. FIN-FSA was given powers to issue regulations and guidance on certain parts of VASP activity. FIN-FSA draft regulation was published for consultation on May 21st. The draft contains regulation on holding and protecting client money and segregation of client money and own funds. Guidance is given on compliance with AML/CFT regulation. The aim is to publish the regulation during summer.

210. Prior to the Act, the FIN-FSA has been working with organizers of ICOs from the point of view of securities markets legislation and financial instruments. The aim has been to identify when the VA is a financial instrument (*i.e.*, transferable security). 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.[26]

211. 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.

---

[24] 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.

[25] . www.finanssivalvonta.fi/en/banks/fintech--financial-sector-innovations/virtuaalivaluutantarjoajat/

[26] . www.finanssivalvonta.fi/en/banks/fintech--financial-sector-innovations/virtuaalivaluutantarjoajat/frequently-asked-questions-on-virtual-currencies-and-their-issuance-initial-coinoffering/

Mexico

212. 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.

213. 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.

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

215. 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.

216. 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.

217. 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

218. 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.

219. 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).

220. 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 onsite 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.

221. 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.

222. 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

223. The United States has a comprehensive and technology-neutral regulatory and supervisory framework in place for regulating and supervising "digital financial assets"[27] 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. 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.

224. 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.

[27] 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.

225. 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.

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

***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, virtualto-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 program, recordkeeping, and reporting measures, including filing suspicious activity reports. The AML requirements apply equally to domestic and foreignlocated 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, 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, 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 issue securities (including, 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 derivative on the security is subject to SEC jurisdiction.

Commodities and Derivatives Activity. In the United States, digital assets may also 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. 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 or certain other derivatives on such commodities. Pursuant to the Commodity Exchange Act and related Regulations, 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 regulatory 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

226. 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) 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 filed by digital asset providers that, 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 foreign bank account, currency and monetary instrument, and currency transaction reports—all of which could contain investigative leads and evidence necessary to deter and prosecute criminal activity associated with digital assets.

227. 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.[28] 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.

228. 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

[28] *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.

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 money laundering as well as foreign-located persons and organizations who violate U.S. law, among other prosecutions relating to digital assets.

229. 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, foreignlocated persons who provide illicit services to, defraud, or steal from U.S. residents may be prosecuted for violations of U.S. law.

230. 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 (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.

International Co-operation is Key

231. 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.

232. 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 foreignlocated 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.

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 riskbased 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 [29]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:

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

   (b) *R.16* – Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information[30] on virtual asset transfers, submit[31] 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.

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.

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.

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

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

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

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[32] 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.

---

[32] 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.