FATF

FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins

June 2020

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 (2020), *FATF Report to the G20,* FATF, France,
www.fatf-gafi.org/publications/virtualassets/documents/report-g20-so-called-stablecoins-june-2020.html

Table of Contents

Executive Summary

1. So-called stablecoins[1] have the potential to spur financial innovation and efficiency and improve financial inclusion. While so-called stablecoins have so far only been adopted on a small-scale, new proposals have the potential to be mass-adopted on a global scale, particularly where they are sponsored by large technology, telecommunications or financial firms. In the same way as any other large scale value transfer system, this propensity for mass-adoption makes them more vulnerable to be used by criminals and terrorists to launder their proceeds of crime and finance their terrorist activities, thus significantly increasing their risk of criminal abuse for money laundering and terrorist financing (ML/TF) purposes.

2. The Financial Action Task Force (FATF) sets international standards to combat money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction. The FATF Standards place specific anti-money laundering and countering the financing of terrorism (AML/CFT) obligations on intermediaries between individuals and the financial system, such as financial institutions. To mitigate the ML/TF risks of virtual assets, the FATF revised its Standards in June 2019 to require virtual asset service providers (VASPs) to implement the full range of preventive measures against ML/TF.

3. In October 2019, the G20 asked the FATF to consider the AML/CFT issues relating to so-called stablecoins, particularly "global stablecoins" (i.e. those with potential for mass-adoption). This report sets out the FATF's analysis of the AML/CFT issues relating to so-called stablecoins. Complementary reports from the Financial Stability Board (FSB), the International Monetary Fund (IMF) consider other implications of so-called stablecoins, including their financial stability and macroeconomic implications.

4. The FATF has found that so-called stablecoins share many of the same potential ML/TF risks as some virtual assets, in virtue of their potential for anonymity, global reach and layering of illicit funds. Depending on how they are designed, they may allow anonymous peer-to-peer transactions via unhosted wallets. These features present ML/TF vulnerabilities, which are heightened if there is mass-adoption.

5. When reviewing current and potential projects, so-called stablecoins appear better placed to achieve mass-adoption than many virtual assets, if they do in fact remain stable in value, are easier to use and are under sponsorship of large firms that seek to integrate them into mass telecommunication platforms.

6. The revised FATF Standards clearly apply to so-called stablecoins.[2] Under the revised FATF Standards, a so-called stablecoin will either be considered to be a virtual asset or a traditional financial asset depending on its exact nature. A range of the entities involved in any so-called stablecoin arrangement will have AML/CFT obligations under the revised FATF Standards. Which entities will have AML/CFT obligations will depend on the design of the so-called stablecoin, particularly the

1 Note on terminology: The FATF considers that the term "stablecoin" is not a clear legal or technical category, but is primarily a marketing term used by promoters of such coins. In order to avoid unintentionally endorsing their claims, this report therefore refers to them as "so-called stablecoins". Those coins called "global stablecoins" in other G20 reports are named "so-called stablecoins with the potential for mass adoption" in this report for the same reason. The FATF uses the defined terms "virtual asset" to refer to crypto-assets and other such digital assets, and "virtual asset service provider" (VASP) to refer to exchanges, wallet providers, and other businesses which provide services relating to virtual assets.

2 FATF, Money laundering risks from "stablecoins" and other emerging assets, October 2019

extent to which the functions of the so-called stablecoin are centralised or decentralised, and what activities the entity undertakes.

7. In a centralised arrangement, one entity governs the arrangement, and may operate the stabilisation and transfer mechanism, and act as the user interface (e.g. by offering custodial wallet and exchange and transfer services). In a decentralised arrangement, there may not be a central entity governing the system, and the stabilisation and transfer functions and user interface may be distributed amongst a range of different entities or be done through software. This is a continuum and a so-called stablecoin may sit anywhere along this spectrum. For example, a stablecoin arrangement may operate the stabilisation centrally, but the user interface may be distributed amongst other VASPs.

8. Importantly, central developers and governance bodies of so-called stablecoins will have AML/CFT obligations under the revised FATF Standards, where they are carrying out the activities of a financial institution or VASP, in addition to the AML/CFT obligations of other entities with AML/CFT obligations, e.g. wallet providers. The central governance bodies of so-called stablecoins are in a unique position to undertake ML/TF risk mitigation, as they determine the functions of the so-called stablecoin, who can access the arrangement and whether AML/CFT preventive measures are built into the arrangement. For example, they could ensure that the access to the transfer system is only possible through AML/CFT-compliant regulated VASPs. Not all so-called stablecoins may have a readily identified central body however.

9. Based on current known models, the FATF consider that so-called stablecoins with potential for mass-adoption will be centralised to some extent, with an identifiable central developer or governance body. The FATF considers that these developers and governance bodies will be, in general, financial institutions (e.g., as a business involved in the 'issuing and managing means of payment') or a VASP (e.g., as a business involved in the 'participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset') under the revised FATF Standards. This is an important control to mitigate the ML/TF risks poses by such so-called stablecoins. Furthermore, there will be a range of other entities with AML/CFT obligations even in a centralised arrangement, including customer-facing exchanges and transfer services and custodial wallet providers.

10. While decentralised so-called stablecoins without such an identifiable central body, prima facie, may carry greater ML/TF risks due to their diffuse operation, the FATF considers that their potential for mass-adoption is lower than centralised arrangements and, therefore, their associated ML/TF risks are smaller (although still present). However, even in a decentralised structure, there could also be a range of entities with AML/CFT obligations, including customer-facing exchanges and transfer services and custodial wallet providers. Importantly, there are functions that may mean an entity has AML/CFT obligations prior to the launch of a decentralised so-called stablecoin, as the process necessary to bring a product to launch is unlikely to be able to be fully decentralised.

11. The FATF considers that the preventive measures required of intermediaries under the revised FATF Standards have worked to mitigate the ML/TF risks posed by so-called stablecoins currently in existence. Accordingly, the FATF does not consider that the revised FATF Standards need amendment at this point in time. Nonetheless, the FATF recognises that this is a rapidly evolving area that must be closely monitored and that jurisdictions must be effectively implementing the revised Standards.

12. In particular, it is important that ML/TF risks of so-called stablecoins, particularly those with potential for mass-adoption and increased anonymity, are analysed in an ongoing and forward-looking manner and are mitigated before such arrangements are launched. As so-called stablecoins could quickly become available globally, with their functions decentralised across multiple jurisdictions, international co-operation between jurisdictions is critical to ensure ML/TF risks are appropriately addressed.

13. The FATF has also identified potential risks which may require further action, including; so-called stablecoins located in jurisdictions with weak or non-existent AML/CFT frameworks (which would not properly implement AML/CFT preventive measures) and so-called stablecoins with decentralised governance structures (which may not include an intermediary that could apply AML/CFT measures) and anonymous peer-to-peer transactions via unhosted wallets (which would not be conducted through a regulated intermediary).

14. Accordingly, the FATF proposes four actions:

a) The FATF calls on all jurisdictions to implement the revised FATF Standards on virtual assets and VASPS as a matter of priority.

b) The FATF will review the implementation and impact of the revised Standards by June 2021 consider whether further updates are necessary. This will include monitoring the risks posed by virtual assets, the virtual asset market, and proposals for arrangements with potential for mass-adoption that may facilitate anonymous peer-to-peer transactions.

c) The FATF will provide guidance for jurisdictions on so-called stablecoins and virtual assets, as part of a broader update of its Guidance. This will set out in more detail how AML/CFT controls apply to so-called stablecoins, including the tools available to jurisdictions to address the ML/TF risks posed by anonymous peer-to-peer transactions via unhosted wallets.

d) The FATF will enhance the international framework for VASP supervisors to co-operate and share information and strengthen their capabilities, in order to develop a global network of supervisors to oversee these activities.

15. To support these actions, the FATF calls on the G20 to lead by example and ensure they have implemented the revised FATF Standards and calls on all other jurisdictions to do the same.

Introduction

16. In October 2019, the G20 asked the FATF to consider the AML/CFT issues related to so-called stablecoins. In line with G20's request, this report:

a) describes what so-called stablecoins are (Section 1);

b) describes the ML/TF risks associated with so-called stablecoins (Section 2);

c) analyses how the revised FATF Standards apply to so-called stablecoins (Section 3);

d) outlines potential residual ML/TF risks associated with so-called stablecoins (Section 4); and

e) sets out the FATF's next steps to ensure the ML/TF risks associated with so-called stablecoins are appropriately mitigated (Section 5).

17. The FATF is the inter-governmental body which sets international standards to prevent money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction. The FATF has agreed that so-called stablecoins are covered by the revised FATF Standards as either virtual assets or traditional financial assets.[3] This followed revisions to the FATF Standards in June 2019 to explicitly apply AML/CFT requirements to virtual assets and virtual asset service providers (VASPs) (see Annex A).

18. So-called 'stablecoins' purport to maintain a stable value relative to some reference asset or assets. This term is not a distinct legal or regulatory classification for a type of asset and is instead primarily a marketing term. Accordingly, this document refers to them as 'so-called stablecoins'.

19. The G20 also mandated the FSB to examine the regulatory issues raised by so-called stablecoins and asked the IMF to consider the macroeconomic implications. While this report is focused on AML/CFT issues, the FATF has worked closely with the FSB, the IMF and other standard-setting bodies in this analysis.

20. Like virtual assets more broadly, the FATF recognises that so-called stablecoins have the potential to spur financial innovation and efficiency and improve financial inclusion. However, they also have the potential to be mis-used by criminals and terrorists for ML/TF purposes, particularly if a so-called stablecoin were to be mass-adopted on a global scale. To ensure these risks are mitigated, it is critical that jurisdictions implement the revised FATF Standards.

3 FATF, Money laundering risks from "stablecoins" and other emerging assets, October 2019

Section 1: So-called stablecoins

21. There is no commonly agreed definition of so-called stablecoins. The FSB considers that so-called stablecoins are a type of crypto-asset '*that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets to other assets*'.[4]

22. So-called stablecoins could be classified as virtual assets under the revised FATF Standards. Virtual assets is the term the FATF uses to refer to crypto-assets and other digital assets that do not function as legal tender.[5] Depending on the design of the so-called stablecoin, it may instead be classified as traditional financial asset (e.g. a security) under the revised FATF Standards or national regulations. As all so-called stablecoins are a type of either virtual or financial asset, they are covered by the revised FATF Standards. This is explained in more detail in Section 3.

23. As their name implies, the key distinguishing feature of so-called stablecoins is that their value is meant to be stable relative to that of an underlying asset or benchmark. The value of a so-called stablecoin may be pegged, for instance, to the value of a fiat currency or a basket of assets that may include fiat currencies, digital currencies, investment securities, commodities and/or real estate. A so-called stablecoin may also employ algorithmic means to stabilise its market value.

24. The characteristics of so-called stablecoins can differ depending on their underlying technology. They can be *permissionless* (where anyone can read and write to the underlying transaction ledger) or *permissioned* (where only selected entities can read and/or write to the transaction ledger). They can also be *public* (where anyone can use the transaction ledger for transactions) or *private* (where only selected entities can initiate transactions). Similarly, so-called stablecoins could be used by anyone (*retail* or *general purpose*) or used only by a limited set of actors, e.g. a selection of financial institutions (*wholesale*).[6]

25. Some proposed so-called stablecoins have been sponsored by large technology, telecommunications or financial firms and seem to have the potential for rapid scaling and mass-adoption. By contrast, so-called stablecoins which already exist have not been widely adopted so far. These proposed so-called stablecoins aspire to quickly reach widespread global adoption, by offering global payment arrangements that are purported to be faster, cheaper and more inclusive than present arrangements; and by leveraging the capital and customer-base of their backers through their integration into pre-existing communication platforms. For the purpose of this paper, these are referred to as *so-called stablecoins with potential for mass-adoption*.[7]

26. So-called stablecoins are different from central bank digital currencies. The revised FATF Standards explicitly exclude central bank digital currencies from the definition of virtual asset, because the revised FATF Standards cover and apply to central bank digital currencies similar to any other form of fiat currency issued by a central bank. Further information on central bank digital currencies is in Annex B.

4 FSB, Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements: Consultative document, April 2020

5 The FATF defines a '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.

6 BIS, Investigating the impact of global stablecoins, October 2019, p. 1

7 These are sometimes referred to as 'global stablecoins'.

Section 2: ML/TF risks of so-called stablecoins

27. The FATF first assessed the potential ML/TF risks posed by virtual assets in 2014 and has since been closely monitoring the evolving risks in this space through regular surveys issued to members of the FATF Global Network, which comprises the FATF, nine FATF-Style Regional Bodies and their respective members.[8] For the purposes of this report, the FATF has also reviewed the current and potential ML/TF risks and vulnerabilities of so-called stablecoins specifically. It is important that ML/TF risks are analysed in an ongoing and forward-looking manner and are mitigated before so-called stablecoins are launched, particularly those with potential for mass-adoption that can be used for peer-to-peer transactions. It will be more difficult to mitigate risks of these products once they are launched.

28. As with the ML/TF risks posed by virtual assets more broadly, the FATF identified *anonymity*, *global reach* and *layering* as being particular ML/TF vulnerabilities for so-called stablecoins. The degree to which these risks materialise depends on the features of the so-called stablecoin arrangement, the extent to which jurisdictions have implemented AML/CFT mitigating measures, and also, critically, on the extent to which there is *mass-adoption* of the so-called stablecoin. As set out above, certain so-called stablecoin proposals seem to have the potential for much greater adoption than pre-existing virtual assets.

29. While the FATF has concluded that stability of value, on its own, does not pose a specific ML/TF risk, there may be ML/TF risks associated with the stabilisation mechanism specific to so-called stablecoins (e.g. by creating new mechanisms for market manipulation). Such risks remain theoretical at this point, but could be the subject of more detailed analysis in the future should they emerge.

Anonymity

30. Anonymity is a major potential ML/TF risk posed by virtual assets. Many virtual assets have public, permissionless, and decentralised ledgers. While the transaction ledger may be accessible to the public, the ledger may not include any customer identification information. There may also not be any central administrator monitoring transactions. Other virtual assets are private and/or permissioned, with only a limited group of entities able to initiate transactions or view and verify the ledger. Some virtual assets, known as privacy coins or anonymity-enhanced coins, have additional cryptographic software that can further obscure transactions. There are also tools available which can be used to further increase the anonymity of transactions (e.g. tumblers and mixers).

31. The revised FATF Standards mitigate the risk posed by anonymity by placing AML/CFT obligations on entities that carry out certain financial activities involving virtual assets (e.g. VASPs or financial institutions). Where a customer uses a VASP to make a transaction, for example, the VASP must identify the customer and maintain transaction records. However, the revised FATF Standards do not explicitly apply to peer-to-peer transactions without the use of a regulated intermediary such as a VASP. For example, private transactions between users with unhosted wallets, where neither is operating as a business. Use of a VASP is not mandatory under the revised FATF Standards, so peer-to-peer transactions without use of a VASP or other

8 In 2014, FATF used the terminology 'virtual currency'. See FATF, Virtual Currencies: Key Definitions and Potential AML/CFT Risks, June 2014.

AML/CFT-obliged intermediary can potentially be used to avoid the AML/CFT controls in the revised FATF Standards.

32. Similar to other forms of payment (such as cash), there is a risk tolerance in the revised FATF Standards for a certain level of anonymous payments for virtual assets. The ML/TF risk for a specific so-called stablecoin, or virtual asset, will depend on how extensive anonymous peer-to-peer transactions with no intermediaries are within an arrangement and whether there are any other AML/CFT controls in place (e.g. transaction monitoring). Currently VASPs claim to offer an easier and more secure service to their users than peer-to-peer transactions. The comparatively greater friction and risk for customers of virtual assets through peer-to-peer transactions acts as a limiting factor on the number and value of peer-to-peer transactions. If unmediated peer-to-peer transactions become easier and more secure, this could prompt a shift away from the use of VASPs. This could increase the number and value of payments not subject to AML/CFT controls and could present a material ML/TF vulnerability if mass-adopted.

Global reach

33. Virtual assets' *global reach* heightens their potential ML/TF risks. Virtual assets can be traded and exchanged via the Internet and can be used for cross-border payments and funds transfer. In addition, virtual assets commonly rely on complex infrastructures that involve several entities, often spread across several jurisdictions, to transfer funds or execute payments. This segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear.

34. Despite this potential, current virtual assets are not widely used as a means of making cross-border payments. This is because they are not widely adopted in all jurisdictions and, in part, because of their unstable value. One of the main use-cases for so-called stablecoins is their purported ability to be a much faster, cheaper and more efficient way of making cross-border transfers, while addressing the volatility issues posed by some virtual assets. Cross-border transfers (like wire transfers or remittance payments) are inherently higher-risk than domestic payments, and are subject to additional AML/CFT measures under Recommendation 16 of the FATF Standards. For virtual assets, this is the 'travel rule', which mandates that VASPs obtain, hold and exchange information about the originators and beneficiaries of virtual asset transfers. However, these rules apply only to transactions involving a VASP or other AML/CFT-obliged entity and do not explicitly apply to unmediated peer-to-per transactions via unhosted wallets.

Layering

35. The fast-moving nature of virtual assets also poses significant ML/TF risks. The ability of quickly exchanging between different virtual assets, a technique known as 'chain-hopping', allows the multiple layering of illicit funds within a short timeframe, thereby allowing a more sophisticated disguise of the origins of funds. Professional ML networks have also appeared to have started exploiting this vulnerability and using virtual assets as one of their means to launder illicit proceeds. So-called stablecoins that can be quickly exchanged for virtual assets or fiat currencies could share this vulnerability.

Potential for mass-adoption

36. The degree to which these risks materialise depends on the features of the specific so-called stablecoin, the extent to which jurisdictions have effectively implemented AML/CFT mitigating measures, and also, critically, on the extent to which there is *mass-adoption* of the so-called stablecoin. Criminals' ability to use a virtual asset as a means of exchange depends on it being freely exchangeable and liquid. In turn, it will be difficult to use as a medium of exchange an asset whose value is highly unstable and which is not widely accepted and trusted. This is in line with the FATF's observation that criminals tend to make use of the more widely-adopted or popular virtual assets in their illicit activities.

37. So far, the FATF has observed that the value of virtual assets involved in most ML/TF appears to be relatively small compared to cases using more traditional financial assets, services and products. Furthermore, it is likely that a relatively small proportion of virtual assets transactions are directly used to conduct criminal or ML/TF activities. While the FATF has noted the abuse of some so-called stablecoins for ML/TF purposes, the FATF has not noted that they have been abused significantly more than virtual assets that do not have stabilisation as a purported feature.

38. The widespread adoption of existing virtual assets as a means of payment by businesses and consumers has been held-back by several factors, including their price volatility, complexity to use, concerns regarding trust and security, and by the lack of general acceptance of virtual assets as a means of payment. While the situation is still evolving, certain proposed so-called stablecoins have the potential to overcome several of these limiting factors. So-called stablecoins are designed to overcome the price volatility issues often associated with many virtual assets. Some proposed so-called stablecoins would build on pre-existing communication and messaging systems, which promise to make them simpler and easier to use (e.g. by being integrated into messaging or social media apps with simple user-interfaces and an existing worldwide user-base of hundreds of millions). The same integration with existing providers could also benefit from a stronger level of trust and security.

39. While price-stability may help a so-called stablecoin reach mass-adoption, it is important to note that a virtual asset without a built-in stabilisation mechanism could also achieve mass-adoption. For example, market conditions (such as more widespread use) or use conditions might reduce price volatility even without an intrinsic stabilisation mechanism. This report considers that a so-called stablecoin is more likely to be mass-adopted than an unstabilised virtual asset, but this does not preclude the possibility that another kind of virtual asset might also achieve this.

Section 3: Application of the revised FATF Standards

Scope of the revised FATF Standards

40. In June 2019, the FATF revised its Standards to explicitly apply AML/CFT requirements to virtual assets and their service providers. These represent the first global AML/CFT regulatory standards for virtual assets and their service providers. The FATF also released new Guidance on the Risk-Based Approach for Virtual Assets and VASPs.[9]

41. The revised FATF Standards define "virtual assets" and "virtual asset service providers" (VASPs), and apply the full range of AML/CFT requirements to them as set out in Recommendation 15 and its Interpretive Note (R.15/INR.15). Jurisdictions must assess the ML/TF risks posed by virtual assets and either permit and regulate virtual assets and VASP activities or prohibit virtual assets and VASP activities. If jurisdictions regulate VASPs as required under the revised FATF Standards, VASPs are subject to the same AML/CFT preventive measures as other financial institutions and AML/CFT-obliged entities, subject to qualifications on the rules for customer due diligence and wire transfers (the 'travel rule'). Jurisdictions must also have supervisory regimes which enable them to license or register VASPs and respond to international co-operation requests regarding VASPs. If a jurisdiction decides to prohibit VASPs, they must take action against non-compliance with the prohibition (see Annex A).

42. Placing AML/CFT obligations on businesses that are intermediaries between individuals and the financial system, such as financial institutions or VASPs, is the key means by which the revised FATF Standards mitigate the ML/TF risks outlined in Section 2. The revised Standards require that relevant intermediaries assess and mitigate their ML/TF risks, including through identifying their customers and transaction monitoring. By doing this, they can deter and detect attempts to misuse their services for ML/TF purposes and ensure that there is sufficient information available for law enforcement to trace illicit transactions.

43. Since their adoption in June 2019, the FATF has been working to ensure prompt and effective implementation of the revised Standards by all jurisdictions and monitoring the ML/TF risks posed by virtual assets. Accordingly, the FATF has undertaken a comprehensive 12-month review of the revised Standards.[10] This review has found that there has been progress by jurisdictions and the VASP sector in implementing the revised FATF Standards. 25 of the FATF's 39 members[11], including 12 G20 members, reported that they have now transposed the revised FATF Standards into their domestic AML/CFT framework. While this is a positive development, all members of the FATF, its Global Network and the G20 must implement the revised FATF Standards as a priority.

9 FATF, Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers, June 2019
10 FATF, 12-month review of the revised FATF standards on virtual assets/VASPs, June 2020
11 The FATF's membership includes 37 jurisdictions and two regional organisations. All 37 member jurisdictions and one regional body responded to the 12-month review.

Application of the revised FATF Standards to so-called stablecoins

44. Depending on how they are set up, each so-called stablecoin arrangement will involve its own different ecosystem of entities. However, there are three broad functions that each so-called stablecoin will typically have:

a) issuance, redemption and stabilisation of value of the coins;

b) transfer of coins among users; and

c) interaction with users (i.e. the user interface).

45. Sitting across these three functions is the governance of the so-called stablecoin arrangement, which establishes the rules governing the stablecoin arrangement. A governance body may also carry out the basic functions of the stablecoin arrangement (such as managing the stabilisation function) or this may be delegated to other entities. They may also manage the integration of the so-called stablecoin into telecommunications platforms or promote adherence to common rules across the stablecoin arrangement.[12]

46. To understand how the revised FATF Standards apply to so-called stablecoins, and whether the revised FATF Standards are sufficient to mitigate the ML/TF risks, the FATF assessed the five largest existing so-called stablecoins[13] (Tether, USD Coin, Paxos, TrueCoin, Dai) and two proposed so-called stablecoins (Libra, Gram). This analysis, as set out below, reflects the FATF's current understanding of these so-called stablecoin arrangements. This report recommends that the FATF release guidance on so-called stablecoins, which would address the practical issues of the application of the revised FATF Standards in greater detail.

47. Depending on how the so-called stablecoin is arranged, a range of businesses in a so-called stablecoin arrangement may have AML/CFT obligations, either as a financial institution or as a VASP. A key determinant is the extent to which the stablecoin arrangement is *centralised* or *decentralised* and whether there are businesses carrying out activities that are captured by the revised FATF Standards. In a centralised arrangement, one entity governs the arrangement, and may operate the stabilisation and transfer mechanism, and act as the user interface (e.g. by offering custodial wallet and exchange and transfer services). In a decentralised arrangement, there may not be a central entity governing the system, and the stabilisation and transfer functions and user interface may be distributed amongst a range of different entities or be done through software. This is a continuum and a so-called stablecoin may sit anywhere along this spectrum. In some cases, there may be both centralised and decentralised elements – e.g. a governance body and third parties with responsibility for specific functions (e.g. exchange or wallet provision). For example, a stablecoin arrangement may operate the stabilisation centrally, but the user interface may be distributed amongst other VASPs. It should be noted, however, that there may be a limit on the extent to which a so-called stablecoin can be fully decentralised prior to launch due to the need for somebody to drive the development and launch of the project.

48. It is clear that the revised FATF Standards apply to so-called stablecoins.[14] The FATF amended its Standards to explicitly apply to virtual assets and their service

12 These functions are explained in further detail in the FSB's report. FSB, Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements: Consultative document, April 2020,.

13 By market capitalisation as of 4 April 2020.

14 FATF, Money laundering risks from "stablecoins" and other emerging assets, October 2019

providers, so as to ensure that there was no gap in the applicability of the FATF Standards. Depending on its structure, a so-called stablecoin would be covered under the revised FATF Standards either as a *traditional financial asset* (e.g. as a security) or as a *virtual asset* (as a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes). The applicable designation will depend on how each jurisdiction has incorporated the revised FATF Standards into their domestic law and the individual characteristics of the so-called stablecoin. However, there should never be a situation where a so-called stablecoin is not covered by the revised FATF Standards. The definition of virtual asset was drafted to be deliberately broad and technology-neutral so that all relevant assets would fall under the revised FATF Standards. The so-called stablecoins analysed are covered by the revised FATF Standards.

49. Any entities within a so-called stablecoin system will have AML/CFT obligations under the revised FATF Standards if they meet the definition of either a *financial institution* or a *VASP*. As set out in INR.15, the AML/CFT obligations on a VASP and a financial institution are largely the same, with specific qualifications in relation to customer due diligence[15] and wire transfer requirements[16] (i.e. the travel rule).

50. Based on the FATF's assessment of different so-called stablecoins, the FATF has concluded that the revised FATF Standards do sufficiently apply to entities involved in these arrangements to mitigate the ML/TF risks. Where they exist and are sufficiently identifiable, central governance bodies will, in general, be AML/CFT-obliged entities. As will other entities in the arrangement, such as exchanges and transfer services and custodial wallet providers. Which entities will have AML/CFT obligations will depend on the stage of development and the design of the so-called stablecoin arrangement, particularly the extent to which the functions of the so-called stablecoin are centralised or decentralised, and what activities an entity undertakes (see Table 1).

51. While decentralised stablecoin arrangements, prima facie, may carry greater ML/TF risks due to their diffuse operation, these risks are limited by what appear to be their apparent natural barriers to mass-adoption (see below). Centralised stablecoin arrangements may have greater potential for mass-adoption, particularly when they are intended to be integrated into mass telecommunication platforms, however they are likely to have more clearly identified entities subject to AML/CFT regulation. In addition, as previously noted, even decentralised products may need to have a centralised control point in the pre-launch stage.

52. At this point in time, the FATF considers that the totality of these obligations has worked to mitigate the ML/TF risks posed by so-called stablecoins. Nonetheless, the FATF has identified residual risks (Section 4). Although these residual risks seem to be currently contained, the FATF should closely monitor them, such that future action can be taken where necessary to keep the risks within acceptable tolerance. In particular, it is important that ML/TF risks of so-called stablecoins, particularly those with potential for mass-adoption, are analysed in an ongoing and forward-looking manner and are mitigated before such arrangements are launched.

15 Recommendation 10, FATF Standards.
16 Recommendation 16, FATF Standards.

Centralised so-called stablecoins

Central developers and governance bodies

53. The central developers and governance bodies of so-called stablecoins are in a unique position to undertake ML/TF risk mitigation, as they determine how the functions of the so-called stablecoin arrangement (e.g. the stabilisation mechanism, transfer of coins and user interface) will operate. They make key design and functionality decisions and they determine the extent to which functions are centralised or decentralised and whether AML/CFT preventive measures are built into a so-called stablecoin. They can also control the access points to the arrangement (e.g. who can participate as an exchange or transfer service or whether a person can only access the system through a VASP) and impose AML/CFT standards setting out expectations or operating requirements for key entities in the arrangement, including exchanges and custodial wallet providers. They are also best positioned to undertake centralised AML/CFT functions, such as transaction monitoring across the so-called stablecoin arrangement. However, depending on the stablecoin arrangement, a range of other businesses may have AML/CFT obligations.

54. The FATF does not seek to regulate the technology that underlies virtual assets or VASP activities or software creators.[17] However, the developers and governance bodies of so-called stablecoins will be AML/CFT-obliged entities if they are carrying out the activities of a financial institution or a VASP. Due to the types of functions necessary for the launch and operations of so-called stablecoins, there will generally be a central administrator or governance body. This is particularly the case for so-called stablecoins *with potential for mass-adoption*, as there typically is need for a body to manage the integration into a telecommunications platform or promote its mass-adoption. This is especially true in the pre-launch phase, as the process of creating and developing an asset for launch is unlikely to be able to be automated. For such so-called stablecoins, the FATF considers that these developers and governance bodies are, in general, a financial institution (e.g., as a business involved in the 'issuing and managing means of payment') or a VASP (e.g. as a business involved in the participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset') under the revised FATF Standards. This is particularly the case if the governance body carries out other functions in the so-called stablecoin arrangement (such as managing the stabilisation function). The exact designation will depend on what functions the body specifically undertakes and each jurisdiction's national law.

55. A central governance body which is a financial institution or VASP under the revised FATF Standards can be held accountable for the implementation of AML/CFT controls across the arrangement and taking steps to mitigate ML/TF risks (e.g. in the design of the so-called stablecoin).[18] This could include, for example, limiting the scope of customers' ability to transact anonymously using the so-called stablecoin[19] and/or by ensuring that AML/CFT obligations of AML/CFT-obliged intermediaries within the arrangement are fulfilled, e.g. by using software to monitor transactions[20] and detect suspicious activity.[21]

17 Paragraph 48, FATF, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, June 2019
18 See Recommendation 15, FATF Standards.
19 See Recommendation 10, FATF Standards.
20 See Recommendation 10, FATF Standards.
21 See Recommendation 20, FATF Standards.

56. Like many virtual assets however, there are so-called stablecoins that do not have a clear central administrator or governance body. There is, *prima facie,* the potential for greater ML/TF risk with decentralised so-called stablecoins. However, the lack of a central body may act as a natural barrier to their potential for mass-adoption, as there is no central body to manage or promote their integration into a telecommunications platform nor promote trust in the system. These so-called stablecoins may also have a centralised body in their pre-launch phase which is responsible for AML/CFT compliance. This is explained in greater detail below.

57. Where there is a central body at any stage of development of the so-called stablecoin, it is critical that national AML/CFT supervisors ensure that the body is taking adequate steps to mitigate the ML/TF risks, before launch where the preparatory activities mean that the entity is a financial institution or VASP, and on an ongoing basis. Under the revised FATF Standards, supervisors must have powers to supervise or monitor, including the power to withdraw, restrict or suspend the AML/CFT-regulated body's licence or registration.[22] There is scope, however, for the FATF to provide Guidance on what approach jurisdictions should take to the supervision of central governance bodies of so-called stablecoins.

58. In summary, developers and governance bodies of centralised so-called stablecoins, particularly those with potential for mass adoption, will likely be a financial institution or VASP under the revised FATF Standards, due with the exact designation depending on the activities they are undertaking and each jurisdiction's national law. There are however residual risks relating to the regulation of such bodies, which are set out in Section 4 below.

Issuance, redemption and stabilisation of value of coins and transfer functions

59. Entities involved in managing the issuance, redemption, stabilisation and transfer functions for the so-called stablecoin may also have AML/CFT obligations under the revised FATF Standards. This will depend on the functions or activities they undertake and whether they are part of the central governance body or standalone entities. In some so-called stablecoins, these functions may be automated and there may not be an entity involved.

60. The entities involved in issuance and redemption may be firms "issuing and managing means of payment" or firms providing or participating in "financial services related to an issuer's offer and/or sale of a virtual asset". Similarly, firms involved in the activities to stabilise the value of a so-called stablecoin may be firms who provide "safekeeping and administration of cash and liquid securities on behalf of other persons", or "safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets" under the revised FATF Standards. The ML/TF risk level of the custodial function itself would vary depending on the manner in which the so-called stablecoin is structured. For example, if the so-called stablecoin holder has a direct or indirect right to redeem the so-called stablecoin for another asset, there could be an ML/TF risk vis-a-vis the custodian or another participant and the redeeming person(s).

61. Depending on the functions they perform, the validator nodes that validate the underlying distributed ledger technology may be VASPs or financial institutions. These entities may be part of the so-called stablecoin governance body or separate

22 Recommendation 27, FATF Standards.

entities. Depending on how the arrangement is established, a few limited participants may be able to be validator nodes or anyone may be able to be a validator node.

Interaction with users

62. There are a range of entities which are intermediaries between individual users and the issuer of the so-called stablecoin, including exchanges and transfer services and custodial wallet services. Businesses acting as exchanges and providing custodial wallet services would be VASPs. The extent to which a user must transact through a VASP (or a financial institution) will depend on the so-called stablecoin. A person may only be able to purchase the so-called stablecoin through a VASP or a financial institution, or they may be able to receive the so-called stablecoin directly (e.g. as a reward for acting as a validator node). Similarly, a person may only be able to transact a so-called stablecoin with a VASP or a financial institution. In other arrangements, there may be an extensive secondary market which enables peer-to-peer transactions that do not involve a VASP or a financial institution. The extent to which anonymous peer-to-peer transactions via unhosted wallets, without involvement of a VASP or a financial institution, can occur in a so-called stablecoin arrangement is a key potential ML/TF risk (see Section 4).

63. Similar to cash, the revised FATF Standards do not directly place AML/CFT obligations on users of virtual assets if they are not financial institutions or VASPs. The revised FATF Standards typically only apply to intermediaries (e.g. banks, money service businesses and VASPs). This means AML/CFT controls only explicitly apply when a person interacts with an AML/CFT-obliged entity. The key control for individuals is the requirement that AML/CFT-obliged entity identify their customers and verify their identity ('customer due diligence'). For users of a so-called stablecoin, they will undergo customer due diligence whenever interacting with a VASP or a financial institution. For example, a person exchanging a so-called stablecoin for fiat currency or a virtual asset through an exchange or a wallet provider, which is acting as a VASP, would undergo customer due diligence. This applies whether the so-called stablecoin is centralised or decentralised or whether it has a potential for mass-adoption of not.

Table 1. Functions subject to AML/CFT obligations in known centralised so-called stablecoin arrangements [1]

Core functions	Specific functions	Is there an AML/CFT-obliged entity (VASP or financial institution)?
Governing the system	*Before establishment:* Setting rules for how to stabilise value, and operate the system and establishing other core functions	Yes [2]
	After establishment: Operating the system and updating rules and potentially other core functions	Yes [3]
Issuance, redemption and stabilisation of value of coins	Issuance and redemption of the coin	Yes
	Management of reserve assets	Depends on arrangement
	Provision of custody for reserve assets	Depends on arrangement
Transfer mechanism(s) [4]	Operation of infrastructure	Depends on arrangement
	Validation	Depends on arrangement
Interaction with users	Storing of asset: *custodial wallet providers*	Yes
	Storing of asset: *non-custodial wallet providers / unhosted wallets*	No (if permitted)
	Secondary market trading: *through exchanges and transfer services*	Yes
	Secondary market trading: *peer-to-peer via unhosted wallets*	No (if permitted)

1. These functions are explained in further detail in the FSB's report. FSB, Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements: Consultative document, April 2020, www.fsb.org/2020/04/addressing-the-regulatory-supervisory-and-oversight-challenges-raised-by-global-stablecoin-arrangements-consultative-document/
2. Based on known models, a centralised so-called stablecoin will, in general. have a governance body and this will have AML/CFT obligations as a financial institution or a VASP. As the so-called stablecoin is in pre-launch phase, it is likely this body will be carrying out a range of functions, including establishing the stabilisation mechanism and promoting its adoption (e.g. through an initial coin offering) (see paragraph 64). They are also in a unique position to undertake ML/TF risk mitigation as they make key design and functionality decisions and they determine the extent to which functions are centralised or decentralised and whether AML/CFT preventive measures are built into a so-called stablecoin (see paragraph 63).
3. See Section 4 for the discussion of residual risks relating to the potential for an arrangement to move to a decentralised model.
4. Those responsible for either effecting a transfer or holding assets are subject to AML/CFT obligations (see interaction with users).

Decentralised so-called stablecoins

64. As noted above, so-called stablecoins can be more or less decentralised. In a fully decentralised so-called stablecoin, there would be no clearly identifiable central governance body, and in the most extreme case no entities of any kind on which AML/CFT preventive measures could be enforced: the governance, stabilisation, and customer interface would be done through software only, with no ongoing management or maintenance after such a system is released. Such a case could pose a significant AML/CFT risk if it were to be mass-adopted, as it would be difficult to apply the risk mitigation measures set out in the revised FATF Standards - in effect becoming a platform for anonymous peer-to-peer transactions via unhosted wallets.

65. However, there are practical and technological limitations which could mean such a radically decentralised scheme is unlikely to achieve the level of ease-of-use, security, or stability which would be necessary to achieve widespread adoption. It is also unclear how such a so-called stablecoin would not be traded through exchanges and transfer services or held in custodial wallets (similar to those virtual assets that do not have a central governance body currently). In addition, some party would have to exist to drive the development and launch of such an arrangement before its

release. If this entity was a business and carried out functions of a financial institution or VASP as set out above, this would create scope for regulatory or supervisory action in the pre-launch phase.

66. So-called stablecoins may also arise which are partially decentralised, but to a less extreme extent. Such so-called stablecoins would most likely include at least some identifiable entities which would be subject to AML/CFT regulation, although exactly which functions are carried out by regulated entities would depend on the design and structure of the so-called stablecoin. As set out above, the FATF considers those with potential for mass-adoption are likely to be centralised to some extent with an identifiable central governance body.

Section 4: Residual ML/TF risks

67. The revised FATF Standards apply to so-called stablecoins. Based on known models, the revised FATF Standards appear sufficient at this stage to mitigate the ML/TF risks involved, where jurisdictions have effectively implemented the revised Standards. Ongoing and forward-looking analysis of the ML/TF risks of proposed and future so-called stablecoins is vital however. It is important that ML/TF risks are addressed before such arrangements are launched, particularly for so-called stablecoins with potential for mass-adoption that can be used for peer-to-peer transactions. It will be more difficult to mitigate risks of those products after they are launched.

68. The effective mitigation of ML/TF risks for so-called stablecoins is contingent on there being strong international co-operation between jurisdictions. Like virtual assets more broadly, so-called stablecoins can be made quickly available to multiple jurisdictions at once. Multiple jurisdictions may have interests in the licencing and registration of proposed so-called stablecoins, particularly if they have potential for mass-adoption. Co-operative supervisory arrangements, such as supervisory colleges or other suitable arrangements, may therefore be necessary. Given that illicit activity involving so-called stablecoins would potentially involve customers and entities established and operating in different jurisdictions, information-sharing and co-ordinated supervisory and law enforcement action is essential to effectively addressing ML/TF activity that might occur through these platforms. The FATF has consequently established a program of work focused on enhancing international co-operation in the supervision of VASPs.

69. The FATF recognises this is an area that must be closely monitored. The FATF has identified three particularly residual risks applicable to so-called stablecoins, which is particularly heightened for so-called stablecoins with potential for mass-adoption.

Risks from anonymous peer-to-peer transactions via unhosted wallets

70. As set out in Section 2, a key potential ML/TF vulnerability for so-called stablecoins is the extent to which they permit anonymous peer-to-peer transactions via unhosted wallets without sufficient mitigating controls. As discussed in Section 3, AML/CFT-obliged entities providing services in a so-called stablecoin arrangement would be required to take steps to mitigate ML/TF risks under the revised FATF Standards, including the risks related to anonymous peer-to-peer transactions.

71. Nonetheless, the FATF recognises that unregulated anonymous peer-to-peer transactions via unhosted wallets is a potential ML/TF risk in the virtual asset market. Since June 2019, the FATF has focused on ensuring that there is prompt and effective implementation of the revised FATF Standards by jurisdictions and the VASP sector. The best way to mitigate the ML/TF risks posed by such disintermediated transactions remains an area of focus and will be considered in further detail by the FATF as part of its ongoing work on virtual assets.

72. A range of tools are available to mitigate the risks posed by anonymous peer-to-peer transactions if national authorities consider the ML/TF risk to be unacceptably high. This includes banning or denying licensing of platforms if they allow unhosted wallet transfers, introducing transactional or volume limits on peer-to-peer transactions or mandating that transactions occur with the use of a VASP or

financial institutions. The mitigation of these risks is more challenging in the case of decentralised governance structure. While authorities may wish to use such tools following the risk-based approach to AML/CFT, they do not form an explicit part of the revised FATF Standards. International co-operation in the development and exercise of these tools will be important.

73. The FATF has conducted a 12-month review of the revised Standards and has decided to conduct a further 12-month review by June 2021. This further review will explicitly consider whether further action should be taken to ensure national authorities have adequate tools to manage the ML/TF risk posed by anonymous peer-to-peer transactions via unhosted wallets. .

Risks from weak or non-existent AML/CFT regulation by some jurisdictions

74. Similar to other AML/CFT-obliged entities, the effective enforcement of supervisory obligations in relation to so-called stablecoins is contingent on the ability and will of their home supervisor to intervene as part of the ongoing registration or licensing process for the financial institutions or VASPs involved with the so-called stablecoin. This is particularly important for so-called stablecoins with potential for mass-adoption, as they could have a much greater global impact. An entity may seek to circumvent its AML/CFT obligations by establishing or operating in a jurisdiction with weak or non-existent AML/CFT controls. By engaging in this regulatory arbitrage, the so-called stablecoin provider could seek to evade the measures in the revised FATF Standards. This perennial vulnerability of regulatory arbitrage is present also in the context of fiat currencies, but is particularly pertinent for VASPs as they may be able to quickly establish and have a global presence.

75. Effective implementation across the FATF's Global Network is critical to combat the risk that VASPs may use jurisdictional boundaries to evade effective supervision and enforcement. The FATF and its Global Network drive implementation and identify high-risk jurisdictions through its peer review process, which comprises mutual evaluations and follow-up processes. For those jurisdictions that the FATF identifies as having strategic AML/CFT deficiencies, the FATF has an additional increased monitoring process. This process could include jurisdictions with weak or non-existent regimes for virtual assets and VASPs. If there is a real risk of regulatory arbitrage occurring, the FATF could consider using this process to specifically target a jurisdiction with poor AML/CFT controls which became a 'safe haven' for VASPs, whether intentionally or negligently.

76. In addition, the revised FATF Standards explicitly permit jurisdictions to require VASPs incorporated in another jurisdiction to be licensed or registered, and subject to their own regulation and supervision, before allowing the VASP to conduct significant business or operations within their territory. If a so-called stablecoin provider were located in a jurisdiction with poor or non-existent AML/CFT controls, other jurisdictions could apply their stronger AML/CFT laws to these providers and other entities within the arrangement. Accordingly, a so-called stablecoin would need to abide by all applicable AML/CFT laws, including those of the jurisdiction in which it is located and into which it offered services. However, enforcement of these rules might be more difficult if the home supervisor of the VASPs has not implemented the revised FATF Standards strongly enough to respond to international co-operation requests.

Risks from so-called stablecoins having a decentralised governance structure

77. At this point in time, it remains likely that there will be a central body that creates and promotes a so-called stablecoin arrangement, particularly if the aim of the arrangement is to be mass-adopted worldwide. This body would likely then be subject to AML/CFT regulation, either as a financial institution or as a VASP. However, the FATF is aware of proposals for establishing so-called stablecoins that, once launched and able to function on their own, would immediately dissolve the entity that created it. That is, they would move from a centralised to a decentralised arrangement. The body that creates and promotes such a decentralised platform would likely qualify as a financial institution or VASP, but such an arrangement would still present risk if supervisors could not intervene in time to ensure adequate AML/CFT protections are built in before release. In those cases, supervisory powers potentially must be exercised before the so-called stablecoin launches, where the preparatory activities mean that the entity is a financial institution or VASP, and otherwise as long as the stablecoin arrangement exists. In addition, other entities involved in the stablecoin arrangement (e.g. exchanges and wallet providers) will continue to have AML/CFT obligations, regardless of whether the central body dissolves.

78. The FATF recognises the need to closely monitor this area for any indication that the Standards would not be sufficient, particularly if a decentralised stablecoin with potential for mass-adoption was being established. As discussed above, it is unclear whether these scenarios would arise based on current models. This possibility raises the importance of the widespread implementation of the revised FATF Standards and co-operation throughout the FATF's Global Network to identify any such indication.

Section 5: Enhancing the global AML/CFT framework for virtual assets and so-called stablecoins

79. The virtual asset sector is fast-moving and technologically dynamic – as evidenced by the emergence of proposals for so-called stablecoins with potential for mass-adoption. While the revised FATF Standards were designed to be technology-neutral, the FATF is mindful of the need to ensure that the revised Standards and its accompanying Guidance effectively respond to any significant changes to the ML/TF risk environment.

80. As set out in this report, the revised FATF Standards apply to so-called stablecoins. However, given the nascent implementation of the revised Standards and the rapid pace of developments in the virtual asset space, the FATF is mindful that further monitoring and assessment is necessary to ensure that the ML/TF risks continue to be appropriately mitigated. Accordingly, the FATF will undertake four actions as set out below. This work program is not specific to just so-called stablecoins; it applies to virtual assets more broadly. Efforts to enhance the AML/CFT response to so-called stablecoins will also enhance the overall global response to virtual assets. The FATF will work collaboratively with the FSB and other global standard-setting bodies to ensure that there is a holistic international response to so-called stablecoins, with AML/CFT integrated into this.

81. **The FATF will promote implementation of the revised Standards by jurisdictions and by the private sector.** The first step to ensuring an effective global response to so-called stablecoins, and virtual assets more broadly, is ensuring that the FATF's pre-existing Standards are transposed into domestic law and operationalised. The global AML/CFT response cannot be fully realised until all jurisdictions have taken appropriate action to understand the ML/TF risks posed by so-called stablecoins and implemented AML/CFT mitigating measures.

82. The FATF calls on members of the FATF and its Global Network to implement the revised FATF Standards as a matter of priority. The FATF calls on the G20 to lead by example and ensure that all members implement the revised FATF Standards. If jurisdictions are implementing regulatory regimes specifically for so-called stablecoins, they should ensure that AML/CFT controls are built into these regimes.

83. The FATF and its Global Network will continue to conducts mutual evaluations to assess jurisdictions' compliance with the revised FATF Standards, which will assist in identifying further potential difficulties or challenges. Jurisdictions which are now undergoing the mutual evaluation and follow-up processes are already being assessed on their implementation of the revised FATF Standards on virtual assets and VASPs. The FATF will also continue to liaise with the private sector to monitor the sector's implementation of the new requirements, particularly the "travel rule" which enables the transfer of important identifying information between VASPs.

84. **The FATF will continue to review the implementation and impact of the revised Standards, and consider whether further updates are necessary**. Concurrently with this report, the FATF completed a 12-month review of the implementation and impact of its revised Standards. This review found there has been progress in implementing the revised FATF Standards and did not identify a need to amend the revised FATF Standards at this point in time. However, the review recognised the need for the FATF to continue to closely monitor this area, particularly

in relation to the ML/TF vulnerabilities relating to anonymous peer-to-peer transactions via unhosted wallets.

85. The FATF has agreed that it will conduct a further review of the impact of its Standards by June 2021. Through this review, the FATF will continue to monitor the ML/TF risks posed by virtual assets, the virtual asset market and so-called stablecoin proposals as they develop and consider whether further action is necessary. The review will consider whether the ML/TF risks posed by so-called stablecoins, including anonymous peer-to-peer transactions via unhosted wallets, are adequately addressed by the revised FATF Standards and, if not, whether further updates are necessary.

86. **The FATF will provide guidance on so-called stablecoins, as part of a broader update of the FATF's Guidance on virtual assets.** The FATF will provide tailored advice to jurisdictions on the risk-based approach to AML/CFT regulation of so-called stablecoins and will address the practical issues outlined above in light of the ongoing rapid developments in this sector. This will consider what tools, powers, skills and expertise supervisors may need to effectively regulate so-called stablecoins and situations where jurisdictions may wish to prohibit a specific so-called stablecoin proposal. This updated guidance will also address other issues the FATF identified in its 12-month review process, including the tools available to jurisdictions to address the ML/TF risks posed by anonymous peer-to-peer transactions via unhosted wallets.

87. **The FATF will enhance the international framework for VASP supervisors to co-operate and share information and strengthen capabilities**. Due to the global reach of virtual assets, effective VASP supervision is contingent on effective international co-operation. As VASP supervision is nascent in many jurisdictions, the FATF is leading work to enhance the international framework for VASP supervision. This forms part of the FATF's work enhancing general supervisory capacity and includes actions to improve information-sharing between supervisors and to build-up the capabilities of the authorities designated to oversee VASP compliance with AML/CFT requirements.

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

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).

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

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.[23] 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.

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

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

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.

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

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.

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[24] on virtual asset transfers, submit[25] 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.

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

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

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

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.

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[26] 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.

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

Annex B. Central bank digital currencies

88. The Committee on Payments and Market Infrastructures and Markets Committee define a central bank digital currency (CBDC) as a "*digital form of central bank money that is different from balances in traditional reserve or settlement accounts*".[27] The concept of CBDCs is sometimes linked to that of so-called stablecoins, as they are representations of a single fiat currency and should, in theory, have a relatively stable value if the currency has a stable value. However, as they are digital representation of fiat currencies and issued by a national government, they should be differentiated from commercial so-called stablecoin proposals. There are three different types of CBDC that vary depending on who has access and on the technology used:

a) digital central bank tokens that can be used by financial institutions (e.g. for interbank and securities settlements);

b) accounts at the central bank for the general public, and

c) digital "cash" that could be used by the general public in retail payments.[28]

89. For FATF's purposes, CBDCs are not virtual assets. The revised FATF Standards explicitly state that virtual assets 'do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations'. The revised FATF Standards however apply to central bank digital currencies similar to any other form of fiat currency issued by a central bank. Therefore, the activities of financial institutions, designated non-financial businesses and professions and VASPs using CBDCs would be covered as if they were using cash or electronic payments.

Risks and risk mitigation for CBDCs

90. With their design at earlier stages, the FATF's understanding of the ML/TF vulnerabilities of CBDCs is less clear. The ML/TF risks of CBDCs will however differ depending on their design.

91. CBDCs could present greater ML/TF risks than cash. CBDCs could be made available to be used by the general public in retail payments or as accounts and, in theory, allow for anonymous peer-to-peer transactions. In this scenario, the CBDC would be acting as an instrument with the liquidity and anonymity of cash, but without the limitations on portability that come with physical cash. A point of comparison might be highly liquid bearer bonds, as these would be potentially high-value bearer instruments. As they would be backed by the central bank of a jurisdiction, they potentially could be widely accepted and widely used. This combination of anonymity, portability and mass-adoption would be highly attractive to criminals and terrorists for ML/TF purposes. As is the case for so-called stablecoins, such ML/TF risks should be addressed in a forward-looking manner before the launch of any CBDCs.

27 Committee on Payments and Market Infrastructures and Markets Committee, Central bank digital currencies, CPMI Papers, no 174, March 2018.

28 BIS, Investigating the impact of global stablecoins, October 2019, p. 29.

92. As the design of CBDCs will determine their risks, there is also the possibility they may have lower ML/TF risks than cash. A wholesale CBDC, for example, that can only be used among licensed financial institutions for interbank settlement may have lower risks than a retail instrument. The risk level, whether higher, lower, or simply different, cannot be determined without more information about the actual design of the product.

93. For ML/TF risk mitigation, this will be led by the issuer of the CBDC (most likely, a jurisdiction's central bank) or the CBDC system operator, if they are not the same. At the design stage of the CBDC, the issuer can make design decisions that reflect and mitigate the ML/TF risks posed by the CBDC. This, for example, could include limiting the ability for anonymous peer-to-peer transactions to occur with the CBDC. Jurisdictions are already required under the revised FATF Standards to identify ML/TF risks relating to new technologies[29] and apply appropriate measures to mitigate those risks.[30] They will also need to consider privacy and data protection implications of such measures.

94. Once a CBDC is established, financial institutions, designated non-financial businesses and professions and VASPs that deal in the CBDC will have the same AML/CFT obligations as they do with fiat currencies or cash. A customer transacting using a CBDC will have the same customer due diligence obligations as if it was an electronic transaction using fiat currency. The issuer of the CBDC (and law enforcement and supervisors) may have greater information on the transactions that are occurring with CBDCs than with physical cash. This is contingent on how the CBDC is designed, whether the users are identifiable and the extent to which activity can be tracked. Both AML/CFT and data protection and privacy concerns are important concerns in the considerations of such features.

29 Recommendation 15, FATF Recommendations.
30 Recommendation 1, FATF Recommendations.

References

BIS, *Investigating the impact of global stablecoins*, October 2019, www.bis.org/cpmi/publ/d187.pdf

FATF, *Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers*, June 2019, www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

FATF, *Money laundering risks from "stablecoins" and other emerging assets*, October 2019, www.fatf-gafi.org/publications/fatfgeneral/documents/statement-virtual-assets-global-stablecoins.html

FATF, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, June 201, www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

FSB, *Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements*: Consultative document, April 2020, www.fsb.org/2020/04/addressing-the-regulatory-supervisory-and-oversight-challenges-raised-by-global-stablecoin-arrangements-consultative-document/.

www.fatf-gafi.org