Electronic Money Association

68 Square Marie-Louise

Brussels 1000

Belgium

info@e-ma.org

www.e-ma.org

Secretariat
Financial Action Task Force
2 Rue Andre Pascale
75775 Paris CEDEX 16
France

23 April, 2021

Dear Sir/Madam

EMA response to FAFT consultation on its draft revised guidance for VASPs

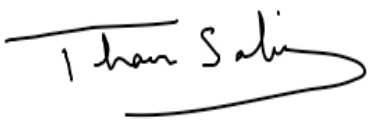
The Electronic Money Association is the trade body for electronic money issuers and innovative payment service providers ("**PSPs**"), and our members additionally include virtual asset service providers -("**VASP**"s) who provide a range of related services such as exchange and custody activities.

Our interest in the activities of VASPs is general, it also extends to the application of DLT to traditional e-money and payments products, and to the novel payment products that exhibit novel attributes, including those of stable coins.

Below are comments in response to the questions and to the provisions of the draft guidance of 19 March 2021.

We are available to address any questions that arise, or to provide any further information.

Yours sincerely



Thaer Sabri
Chief Executive Officer

Electronic Money Association

The Electronic Money Association (EMA) is the trade body representing electronic money issuers and payment service providers. A list of EMA members is provided at Annex 1 to this document.

Comments on paragraphs 1-46

- **Paragraph 36 risk elements relating to VASPs:** paragraph (i) suggests that transactions to and from non-obliged entities or where P2P transactions have occurred are indicators of heightened risk. We suggest distinguishing P2P transactions from those where unregulated VASPs or unobligated entities are involved. The majority of P2P transactions will be legitimate transactions that do not give rise to increased risk. We understand that the majority of P2P transactions are in fact first person transfers of VAs for the purpose of safekeeping.

- **Paragraph 37 risk elements relating to VASPs**: the following statement is made: "Some countries may decide to prohibit or limit VA activities or VASPs, and those VA activities carried out by non-obliged entities". We caution against limiting P2P transactions, and suggest distinguishing those from transactions relating to unregulated VASPs. The majority of P2P transactions are legitimate transactions that take advantage of the distributed nature of the technology and enable efficiencies and cost savings to be made.

- **Paragraph 46 reference to stable coins:** we concur that the term 'stable coin' encompasses a range of products with differing attributes. We encourage the FATF however to adopt this term and discontinue the 'so called' pronoun.

Conclusion: P2P transactions are a legitimate type of user functionality and do not merit classification as higher risk.

1. **Does the revised Guidance on the definition of VASP (paragraphs 47-79) provide more clarity on which businesses are undertaking VASP activities and are subject to the FATF Standards?**

- **Paragraph 57** suggests that the owner or operator of software is a VASP, and further adds that those conducting business development may themselves be VASPs. We suggest that only the entity that carries out an exchange or transfer etc. by way of business should be regarded as a VASP, and parties that conduct activities that are elements of a VASP activity, whether business development, software development etc. should be subject to the oversight of the VASP itself. Independent business development or other service providers are not regulated when offering services to other types of obliged entities and the merits of regulation here have not been adequately made.

A similar difficulty arises when classifying owners or operators of entities as VASPs themselves; particularly where ownership may be distributed amongst a class of token holders, or governance is facilitated in this way. It would not be equitable to suggest that shareholders in an FI could themselves have to be financial institutions.

It may be that the nature of distributed services necessitates a novel approach to AML regulation, and a reconsideration of where the points of influence lie in a given value chain.

- **Paragraph 60**: the question of the role of governance as a trigger for regulation. Where governance is undertaken by a community of individuals, it will be difficult to suggest each individual token holder or node provider should be regarded as a VASP.

Conclusion: the governance and operation of DLT systems can be highly democratized. It is not proportionate to regard each party contributing to such roles as a VASP in its own right.

Is further guidance needed on how the FATF Standards apply to various business models, as stated in paragraphs 56-59? How should the Guidance further address the challenges in applying the definition of VASP to businesses which decentralize their operations across multiple parties?

Developers of DeFI applications develop software as a business similar to developers of HTPP based applications; they do not provide financial services and they do not have access to data that would enable them to comply with KYC, monitoring and reporting requirements. In a DeFi system, there is no party that approves transactions, there is no intermediary institution that customers transact with, there are no necessary permissions and no party other than the user has control over an asset. Furthermore, DeFi systems are closed systems, requiring users to under KYC on entry and exit, which reduces their utility for ML/CTF purposes. We oppose the suggestion in paragraph 57 that “the owner/operator [of a DApp] is likely to be a VASP, even if other parties play a role in the service or portions of the process are automated.” Any owner/operator of a DApp should only be a VASP if they engage as a business in one of the five activities of a VASP. Given the way DeFi is structured, this is unlikely and we therefore suggest the removal of this statement. This would be in line with the

distinction made in paragraph 68 between software developers and those who provide a financial service.

Conclusion: Developers of DeFi applications should not fall under the definition of a VASP, as they do not provide financial services.

Is more guidance necessary on the phrase 'for or on behalf of another natural or legal person' in the FATF definition of VASP? What are the challenges associated with applying the business-customer relationship concept in the VASP context?

Do the clarifications on the 'expansive' approach to the definition of VASP in identifying and policing the 'regulatory perimeter' for VASPs provide countries and the private sector with enough guidance? What additional clarity can be given to make the perimeter clearer?

The concept of regulatory perimeter suggests a clear boundary that separates services in scope of regulation for those outside of scope. Such a boundary is important in order to provide legal certainty to industry participants and ensure the justiciability of regulatory decisions. By providing jurisdictions with a wide space of discretion where to draw the boundary (paragraph 76), the 'expansive' approach to the VASP definition adopted by the FATF does away with these legal values. Statements such as this in paragraph 76 – "where customers can access a financial service, it stands to reason that some party has provided that financial service, even if the act of providing it was temporary or shared among multiple parties" – have no place in legal guidance, which should be aimed at concrete business models rather than be speculative. The 'expansive' approach risks stifling innovation, economic growth and financial inclusion; it also risks the further decentralisation of financial services in order to escape a regulatory perimeter that is unpredictably wide.

Conclusion: The 'expansive' approach to the definition of VASP is thought to be in appropriate for a regulatory regime and may ultimately prove to be counterproductive.

2. What are the most effective ways to mitigate the money laundering and terrorist financing (ML/TF) risks relating to peer-to-peer transactions (i.e., VA transfers conducted without the use or involvement of a VASP or other obliged entity, such as VA transfers between two unhosted wallets) (see paragraphs 34-35 and 91-93)?

- **How are peer-to-peer transactions being used for ML/TF purposes and what options are available to identify how peer-to-peer transactions are being used? What role and implications (e.g., benefits) do peer-to-peer transactions and unhosted wallets have in VA ecosystems?**
- **What specific options are available to countries and VASPs to mitigate the ML/TF risks posed by peer-to-peer transactions?**
- **Are the risk mitigation measures proposed in the Guidance in paragraphs 91-93 appropriate, sufficient and feasible?**

Paragraphs 179-180 require VASPs that send or receive VAs from an unhosted wallet to obtain identification information about the owner of that wallet from their customer. This is likely to create some friction in the transaction and may be resisted by some customers on privacy grounds. Furthermore, the information will not be verified. It may be preferable to require VASPs to record detected data relating to such wallets and when required, make this available to law enforcement for investigations.

Requiring customers to provide information about unhosted wallets they transact with may also deter them from using regulated VASPs in the first instance, encouraging them to move their VAs to their own unhosted wallets. This will push transactions out of the regulated financial system, with an associated loss of the ability to apply controls, such as monitoring and suspicious activity reporting.

Conclusion: VASP customers should not be required to provide identifying information related to unhosted wallets. They may not submit accurate information and the burden of this requirement may deter some customers from using regulated VASPs in the first instance.

3. Does the revised Guidance in relation to the travel rule need further clarity (paragraphs 152-180 and 256-267)?

- **Are there issues relating to the travel rule where further guidance is needed? If so, where? Please provide any concrete proposals.**

While under IN16 4(a), credit, debit and prepaid cards are exempted from travel rule requirements if they are used for the purchase of goods and services, VAs are not currently included in this exemption. This is even though VAs that are used to purchase

goods and services give rise to a lower risk of TF. We therefore recommend that an equivalent exemption be introduced.

Conclusion: VAs should benefit from an exemption from the travel rule requirements where VAs are used to purchase goods or services.

- **Does the description of counterparty VASP due diligence clarify expectations, while remaining technology neutral and not prescribing how VASPs must undertake this process (see paragraphs 172-177 and 261-265)?**

  We strongly oppose the requirement in paragraph 172 for VASPs to undertake due diligence on counterparties. This requirement imposes similar obligations to those that apply to correspondent banking relationships (such as assessing the counterparty's AML systems and controls and confirming that these are subject to independent audit (paragraph 264)), but is in fact separate and additional to those obligations - as paragraphs 146-147 demonstrate. There is no legal basis for this requirement in Recommendation 16, which does not seek such obligations in relation to any other type of financial institution. It does not therefore accord with the FATF's principle of consistent regulation for functionally similar services (paragraph 22).

  VASPs and their counterparties usually act similarly to payment service providers serving their own customers; except in limited circumstances where the correspondent banking analogy could be applied, they do not act as agents for each other. Therefore, there is also no AML/CTF basis for the requirement, which singles out VASPs amongst all obligated entities and adds unnecessary complexity to the travel rule regime.

  Conclusion: The additional requirement applying to VASPs under the travel rule to identify counterparties should be removed, as it has no basis in Recommendation 16.

4. Does the revised Guidance provide clear instruction on how FATF Standards apply to so-called stablecoins and related entities (see Boxes 1 and 4 and paragraphs 72-73, 122 and 224)?

- **Paragraph 73**: Under paragraph 73, the central governance body of a stablecoin would be subject to AML/CFT regulations as either a financial institution or as a

VASP under point (v) of the VASP definition. It is not clear, however, whether a central governing body would and should be in scope of regulation as a VASP, as it may not issue and manage a means of payment, nor be involved in financial services relating to issuance.

In this respect, paragraph 73 specifically refers to involvement in the stabilisation mechanism and to "decision-making authority over structures that affect the inherent value of a VA" as aspects of governance bodies that warrant regulation under point (v) of the VASP definition, "depending on the extent of the influence each party has." While these functions arguably carry some prudential risk, it is unclear how they are relevant from a ML/TF risk perspective.

Conclusion: The inclusion of central governance bodies of stablecoins in the scope of regulation should be re-assessed in light of ML/TF risk.

- The guidance further states **at paragraph 73** that "each natural or legal person constituting the governance body could also be a VASP depending on the extent of the influence it may have." The inclusion of members of governance bodies is disproportionate, given the FATF's proposals to regulate the governance bodies themselves. Furthermore, this provision singles out entities involved in stablecoins amongst other financial institutions. Additionally, it is unclear why entities that are not themselves carrying out activities that fall within the scope of the definition of a VASP are captured merely on account of their influence over a VASP. After all, such influence is already addressed through fitness and probity regimes and the provisions on beneficial ownership.

Conclusion: Members of central governance bodies of stablecoins should not be VASPs in their own right.

- **Paragraphs 89-90** again single out stablecoins amongst all other regulated financial products, contravening the principle of consistent regulation for functionally similar services (paragraph 22). They suggest that central governance bodies of stablecoins may be regulated early, i.e., in the product development stages. Such early regulation would likely stifle financial innovation and compromise confidentiality in R&D processes. Other options exists, such as regulatory sandboxes, and these are thought to be preferable if collaboration with regulators is sought.

Conclusion: We advise against the early regulation of central governance bodies of stablecoins during product development stages.

- **Paragraphs 90 and 73** provide that a central governance body "can be held accountable for the implementation of AML/CFT controls across the arrangement and for taking steps to mitigate ML/TF risks (e.g. in the design of the so-called stablecoin)." However, unlike NPPS, who have control over their ecosystem, central governance bodies of stablecoins are not able to police the entire system, given that third parties such as other regulated VASPs or developers may participate in and build on its basic structures.

  Furthermore, central governance bodies have no sight of transactions and are therefore unable to carry out transaction monitoring and suspicious activity reporting.

Conclusion: If at all, central governance bodies should only be held accountable for their own processes, not for all entities within the stablecoin ecosystem.

- **Is the revised Guidance sufficient to mitigate the potential risks of so-called stablecoins, including the risks relating to peer-to-peer transactions?**

At several points in the guidance (e.g., para. 224), statements are made that effectively describe stablecoins as higher risk. While mass adoption and any stabilisation mechanism are mentioned in this regard, little evidence or reasoning of how these factors are thought to increase ML/TF risk has been provided and their benefits have not been considered. For instance, the centralisation and ready availability of data associated with mass adoption may offer a number of opportunities for the prevention of ML that smaller or more fragmented schemes lack. It is presumably for this reason that mass adoption is not a risk factor generally referred to in the FATF standards. Similarly, it is not clear where the particular ML risks lie in respect of any stabilisation mechanism. Other than with VAs whose value fluctuates, stablecoins afford very narrow margins for gains made from trading.

The statements also contravene the FATF's own stated principle that it does not prejudge a sector as higher risk (para. 28). We recommend that they are replaced with

a reference to a risk-based approach that takes account of the specific characteristics of each stablecoin proposition.

Conclusion: The guidance should not describe stablecoins as higher risk.

5. Are there any further comments and specific proposals to make the revised Guidance more useful to promote the effective implementation of FATF Standards?

Many competent authorities currently face a backlog of VASP licence applications. Para. 117 suggests that, where applicants have not yet stparagraph 122arted trading, competent authorities could "consider beginning with the easiest applications first and then moving on to the higher risk or more complex applicants thereafter." This suggests preferential treatment on the basis of an application's complexity and in our view constitutes undue interference by the FATF in commercially sensitive licencing processes. In order to remain neutral and treat all applicants equally, applications should be processed in the order in which they are received.

Conclusion: Licence applications should be processed in the order in which they are received.

Annex 1: List of EMA members as of April 2021

- AAVE LIMITED
- Account Technologies
- Airbnb Inc
- Airwallex (UK) Limited
- Allegro Group
- American Express
- Azimo Limited
- Bitpanda Payments GmbH
- Bitstamp
- BlaBla Connect UK Ltd
- Blackhawk Network Ltd
- Boku Inc
- CashFlows
- Circle
- Citadel Commerce UK Ltd
- Contis
- Corner Banca SA
- Crosscard S.A.
- Crypto.com
- Curve
- eBay Sarl
- ECOMMPAY Limited
- Em@ney Plc
- emerchantpay Group Ltd
- ePayments Systems Limited
- Euronet Worldwide Inc
- Facebook Payments International Ltd
- Financial House Limited
- First Rate Exchange Services
- FIS
- Flex-e-card
- Flywire
- Gemini
- Globepay Limited
- GoCardless Ltd
- Google Payment Ltd
- HUBUC
- IDT Financial Services Limited
- Imagor SA
- Ixaris Systems Ltd
- Modulr FS Europe Limited
- MONAVATE
- Moneyhub Financial Technology Ltd
- MuchBetter
- myPOS Europe Limited
- OFX
- OKTO
- One Money Mail Ltd
- OpenPayd
- Optal
- Own.Solutions
- Oxygen
- Park Card Services Limited
- Paydoo Payments UAB
- Paymentsense Limited
- Payoneer
- PayPal Europe Ltd
- Paysafe Group
- Plaid
- PPRO Financial Ltd
- PPS
- Remitly
- Revolut
- SafeCharge UK Limited
- Securiclick Limited
- Skrill Limited
- Snowy Pay Ltd.
- Soldo Financial Services Ireland DAC
- Square
- Stripe
- SumUp Limited
- Syspay Ltd
- Token.io
- Transact Payments Limited
- TransferMate Global Payments
- TransferWise Ltd
- TrueLayer Limited
- Trustly Group AB
- Uber BV
- Vitesse PSP Ltd
- Viva Payments SA
- WEX Europe UK Limited
- Wirex Limited
- WorldFirst
- WorldRemit LTD