Crypto Council for Innovation

The premier global alliance advancing crypto innovation.

CCI Response to European Banking Authority (EBA) public consultation on guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under Regulation (EU) 2023/1113 ("The Travel Rule Guidelines") February 26, 2024

The Crypto Council for Innovation (CCI) welcomes the European Banking Authority's (EBA) consultation on its guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under the Transfer of Funds (TFR) Regulation (EU) 2023/1113 (hereafter the Guidelines).

Whilst we broadly support the EBA's overarching objective, namely to strengthen the European Union's AML/CFT regime by ensuring a common understanding by all financial institutions and national competent authorities (NCAs) on how to detect and manage the transfer of funds and crypto-assets lacking the required information on the payer/originator and the payee/beneficiary, we welcome the opportunity, via this submission, to make some targeted comments in relation to one specific issue: the approach toward self hosted wallets (SHWs).

High-level summary of CCI's position:

- **Support proportionate, risk-appropriate AML requirements for CASPs with regards to self-hosted wallets.** Given the significant, recent political agreement reached in the EU's revised AML package, in particular the Anti Money Laundering Regulation (AMLR), which requires a risk-based approach to money laundering and terrorist financing (ML/TF) risks, we believe the language of the Guidelines should fully align with the risk-based emphasis in the EU co-legislators' political agreement in the primary legislation in the AMLR.[1] We are concerned that the Guidelines neglect to include the nuanced text of the TFR level 1 legislation and the recent stance taken by the co-legislators in the AMLR on these same issues that calls for mitigating measures commensurate with the specific risks CASPs identify in their customers' exposure to SHWs.

- **The EBA Guidelines should not stifle and constrain positive innovation occurring around SHWs that supports and even enhances AML/CFT compliance goals.** The digital asset industry is developing products and services involving SHWs that include innovative illicit finance risk management tools and approaches. Financial authorities, regulators and supervisors

[1] Anti-money laundering: Council and Parliament strike deal on stricter rules, https://www.consilium.europa.eu/en/press/press-releases/2024/01/18/anti-money-laundering-council-and-parliament-strike-deal-on-stricter-rules/#:~:text=The%20provisional%20agreement%20on%20an,activities%20through%20the%20financial%20system

in the EU should ensure that the TFR language introduced does not inadvertently restrict the measures CASPs can use to comply with the provisions in and objectives of the TFR.

Response to Question 1: Do you agree with the proposed provisions? If you do not agree, please explain how you think these provisions should be amended, and set out why they should be amended. Please provide evidence of the impact these provisions would have if they were maintained as drafted'?

We believe that some of the provisions would benefit from being revised in order to enhance consistency with broader EU legislation and to provide legal certainty for those firms covered by the scope of the Guidelines. Our key concern is on the misalignment between the EBA's guideline 8.2.2 (paragraph 67) and the text of the Article 19(a) in the currently applicable AML Directive (AMLD V), as revised by the TFR. This misalignment also threatens to undermine the beneficial innovation in risk management services around SHWs in the digital asset ecosystem. Article 19(a)[2] states:

Member States shall require crypto-asset service providers to identify and assess the risk of money laundering and terrorist financing associated with transfers of crypto-assets directed to or originating from a self-hosted address. To that end, crypto-asset service providers shall have in place internal policies, procedures and controls. Member States shall require crypto-asset service providers to apply mitigating measures commensurate with the risks identified. Those mitigating measures shall include one or more of the following:

(a) ***taking risk-based measures** to identify, and verify the identity of, the originator or beneficiary of a transfer made to or from a self-hosted address or the beneficial owner of such originator or beneficiary, including through reliance on third parties;* (emphasis added).

However, paragraph 67 of the guidelines[3] states:

*Where the crypto-asset transfer is not made from or to another CASP or any other obliged entity, but from or to a self-hosted address, in order to obtain the required information on the originator or beneficiary, the beneficiary's CASP and originator's CASP respectively, **should collect the information from their customer.** The beneficiary's CASP and originator's CASP should use suitable technical means to cross-match data, including blockchain analytics and third party data providers, for the purpose of identifying or verifying the identity of the originator or the beneficiary.* (emphasis added).

Although collecting the information from the customer to identify the SHW originator or beneficiary of a transaction may be possible and appropriate in some circumstances, it may not always be the case. There

[2] Anti Money Laundering Regulation (EU) 2023/1113 (AMLR), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1113

[3] Guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under Regulation (EU) 2023/1113, https://www.eba.europa.eu/sites/default/files/2023-11/cc8eb1e9-df10-4517-81a1-de4a8c9d0360/Consultation%20paper%20on%20draft%20travel%20rule%20Guidelines%20under%20Regulation%20%28EU%29%202023_1113.pdf

are some scenarios where the CASP's customer may not typically acquire a transaction counterparty's name, such as when receiving payments for goods or services. Many retail businesses–both online and brick and mortar stores–accept crypto-assets directly from customers.[4] In some cases, customers may be paying through a SHW. Also, while some CASPs do offer SHW software, these SHWs are not part of the custodial wallets the CASPs manage on behalf of customers and thus, CASPs do not have KYC information on those users. We understand and appreciate that EU regulations around these types of transactions and activities are still in the process of being considered - be it in the conclusion of the technical trilogues on AMLR, the EU's payments package (PSD/PSR) or indeed in the European Commission's MiCA mandate to consider, inter-alia, decentralization, of which SHWs are a fundamental part. The language of the AMLR in Article 19(a) is more suitable than para 67 of the Guidelines as it provides variability in how CASPs identify customers' SHW counterparties, depending upon the risks of those transactions (risk-based approach). However, our reading of the draft guidelines appear to eliminate that optionality.

Because data on permissionless blockchains are intrinsically public, it is important to maintain privacy around the personal identity information of users transacting in blockchain environments. The preservation of privacy, besides being a fundamental value within the EU, protected by legislation, is foundational to a well-functioning internet and necessary to support user confidence of blockchain technology and to spur ongoing innovation. Privacy and compliance do not have to be mutually exclusive. It is important to note that the digital asset industry is building various technical solutions and services relating to SHWs in order to mitigate ML/TF risks and support AML/CFT and sanctions compliance goals. For example, there is significant innovation occurring around digital identity and credentials that could be integrated with SHW transactions. These technologies are in development and could improve how financial institutions verify customer identification and source of funds in the future.

We urge the EBA not to preemptively hinder the development of new, innovative private sector AML/CFT and sanctions compliance solutions around SHW by constructing the TFR Guidelines in a manner that undermines such innovation.

We therefore recommend amending paragraph 67 as follows:

Where the crypto-asset transfer is not made from or to another CASP or any other obliged entity, but from or to a self-hosted address, in order to obtain the required information on the originator or beneficiary, the beneficiary's CASP and originator's CASP respectively, should ~~collect the information from their customer.~~ take risk-based measures to obtain the necessary information. The beneficiary's CASP and originator's CASP should use suitable technical means to cross-match data, including blockchain analytics and third party data providers, for the purpose of identifying ~~or verifying~~ the identity of the originator or the beneficiary.

Instead of requiring verification for SHW transactions below 1,000 EUR, we recommend EBA align with the AMLR TFR's language in Articles 14(5) and 16(2), requiring CASPs to *obtain and hold* originator and beneficiary identification information.[5] We recommend EBA require verification only when

[4] Who accepts Bitcoin in 2024?, https://cryptonews.com/guides/who-accepts-bitcoin.htm
[5] See AMLR, Articles 14(5), 16(2)

specifically referring to transactions over 1,000 EUR. It states clearly in the TFR Recital 39, "In the case of a transfer to or from a self-hosted address, the crypto-asset service provider should collect the information on both the originator and the beneficiary, usually from its client. A crypto-asset service provider should in principle not be required to verify the information on the user of the self-hosted address. Nonetheless, in the case of a transfer of an amount exceeding EUR 1 000 that is sent or received on behalf of a client of a crypto-asset service provider to or from a self-hosted address, that crypto-asset service provider should verify whether that self-hosted address is effectively owned or controlled by that client."[6]

In addition, ownership and control of SHWs is also covered by the AMLR with a mandate for the European Commission to explore further. Therefore, it is premature for EBA to hardwire overly prescriptive rules in these Guidelines which would seem to have been superseded somewhat by the recent agreement by legislators on the AMLR package.

To elaborate, CASPs should have discretion to manage the risks through the verification of self-hosted wallet address ownership for transactions exceeding 1,000 EUR, as set out in paragraph 69 of the draft guidelines, which at present reads:

Where the amount of a transfer from or to a self-hosted address exceeds 1 000 EUR, the originator's CASP and beneficiary's CASP should verify whether the self-hosted address is owned or controlled by the originator and beneficiary, respectively, by using suitable technical means, ***which include at least two of the following:***

In line with the wider principles of our comments - that CASPs should retain some variability in implementation, taking as set out in the TFR a risk-based approach that includes consideration of the specific transaction - **we recommend that the proposal in paragraph 69 is revised**, so that dual or more verification of ownership is recommended only for cases where it proves necessary. This would enable a better balance between risk-management, innovation, and compliance burden.

We recognise that such a change would also require updating paragraph 71, which at present acknowledges that, if two methods on their own are not reliable enough to ascertain ownership or control, a combination of more methods should be used. In this instance, we would recommend that CASPs are encouraged that, where they cannot ascertain ownership or control with one or more methods, they use a combination of methods.

We therefore recommend amending paragraphs 69 and 71 as follows:

(69) Where the amount of a transfer from or to a self-hosted address exceeds 1 000 EUR, the originator's CASP and beneficiary's CASP should verify whether the self-hosted address is owned or controlled by the originator and beneficiary, respectively, by using suitable technical means, ***which, depending on relevant risk of the transaction, may include the following:***

[6] *id*. Recital 39

*(71) **Where one method on its own is** not sufficiently reliable to ascertain the ownership or controllership of a self-hosted address, the CASP should ensure that a combination of ~~more~~ methods is used.*