

Response to European Banking Authority (EBA) public consultation on amendments to its Guidelines on money laundering and terrorist financing (ML/TF) risk factors

The Crypto Council for Innovation (CCI) welcomes the European Banking Authority's (EBA) [consultation](#) on its amendments to its Guidelines on money laundering and terrorist financing (ML/TF) risk factors (hereafter the Guidelines).

Whilst we broadly support EBA's overarching objective, namely to extend the scope of these Guidelines to crypto-asset service providers (CASPs), we welcome the opportunity via this submission to make some targeted comments in relation to two specific issues: i) self hosted wallets (SHWs) and ii) enhanced customer due diligence (EDD).

High-level summary of CCI's position:

- **Support for proportionate, risk-appropriate AML requirements for CASPs:** We understand and support EBA's extension of its Guidelines to CASPs. Given the already comprehensive provisions in the recently published [Transfer of Funds Regulation](#) (TFR), which constitutes the EU's implementation of the travel rule, and the current, on-going negotiations to revise the EU's broader AML rules, we believe the Guidelines need to be consistent with these other frameworks. Ensuring proportionality and a risk-based approach are essential in order to effectively tackle ML/TF.
- **We disagree with EBA's inference that SHWs are de facto considered to increase AML risk.** In addition, we contest this assumption when it comes to SHWs utilizing privacy enhancing techniques, bearing in mind that many data protection authorities actually encourage the use of privacy enhancing techniques for GDPR purposes.
- **We remain concerned by the inferred presumption that EDD is always needed for SHWs.** We see a risk that such obligations could trickle down to SHW developers, with broader negative repercussions for open source and decentralized solutions.

The rest of our short submission seeks to provide a bit more background context and detail around these concerns noted above, particularly in relation to questions 6 and 9 (Guidelines 8 and 21). We hope EBA finds this submission helpful and we remain at your disposal for further discussions as you finalize these Guidelines.

Response to Question 6 of the consultation: Do you have any comments on the proposed changes to Guideline 8?

We have some concerns about the amendments to Guideline 8: Sectoral guideline for correspondent relationships, in particular amendments to customer risk factors in 8.6 letter d). In general, the amended d implies that there are automatically higher levels of ML/TF risk' where 'the respondent conducts "significant" (undefined): 'business on behalf of CASPs which allow transfers to and from self-hosted addresses'.

SHWs leave ultimate ownership and control of assets with the asset owner, removing exposure to potential risk such as capitalization/misappropriation risk, via centralized exchanges/custodial wallets. We believe self-hosted wallets should not be seen as synonymous with anonymity: there is a clear distinction between wallets specifically designed to obfuscate transactions and self-hosted wallets. Furthermore, this does not recognise the importance and critical role of SHWs, which many investors choose as their preferred custody solution. SHWs are privacy protective but also allow for detection of illicit finance and other harmful activity through transaction monitoring and wallet screening. SHWs are associated with open, public blockchains and empower individuals to manage their own digital assets. The EBA's current wording of the guidelines fails to acknowledge the distinction between wallets, or the benefits to investors and individuals.

Moreover, the transparency which is built into transactions on public blockchains makes a significant contribution to the integrity of crypto ecosystems. Technological solutions can be used to identify transactions and associated wallet addresses, which ensures effective AML/TF compliance is possible.

CCI recommendation to EBA: deletion of guideline 8.6 d iv. business on behalf of CASPs which allow transfers to and from self-hosted addresses.

Response to Question 9: Do you have any comments on the proposed changes to Guideline 21?

New Guideline 21: Sectoral guideline for crypto asset services providers (CASPs)

Whilst we recognise and support the intention of seeking to enumerate risk factors in relation to CASPs, we would make a general observation that the provisions in guideline 21 are significantly more detailed and prescriptive than provisions in earlier iterations applicable to a broader range of financial institutions.

In short, we strongly feel that consumer due diligence requirements for CASPs should not fundamentally differ from those for traditional financial services, thereby ensuring fair competition and regulatory consistency under the principle 'same risk, same regulatory outcome' principle.

We are particularly concerned about the EDD requirements in guideline 21.12 d iii, where we believe the EBA may be inferring that transactions involving self-hosted addresses, peer-to-peer cryptocurrency exchange platforms and DeFi applications are inherently high risk for ML/TF.

We also are concerned that the proposed wording could be interpreted to convey that CASPs "must" apply additional EDD measures such as obtaining evidence of the source of funds or cryptoassets for transactions involving cash/crypto exchanges, cryptoasset transfers, or exchanges involving mining, airdrops, staking

rewards, ICOs, or crypto lending protocols (as per amended guideline 21.12 d ii) or for 'the transfer of a customer's crypto assets from one exchange to another or to a self-hosted address' (as per amended guideline 21.12 d iii). We believe this goes beyond requirements set out in the TFR.

It is crucial to strike a balance between robust AML/CFT measures and fostering an environment that encourages technological advancements and the responsibly sustainable growth of the crypto industry.

CCI Recommendation: amend the first paragraph of guideline 21.12 as follows:

21.12. Where the risk associated with a business relationship or occasional transaction is increased, CASPs ~~must~~ shall apply EDD measures pursuant to Article 18 of Directive (EU) 2015/849 as set out in Title I. In addition, CASPs ~~should~~ may apply one or all of the following EDD measures: