EFA response to the EBA Consultation on revised Guidelines on money laundering and terrorist financing (ML/TF) risk factors (EBA/CP/2023/11)

The European Fintech Association (EFA) welcomes the EBA's proposal on amendments to its Guidelines on money laundering and terrorist financing (ML/TF) risk factors to include CASPs.

The EFA fully supports a harmonized ML/TF Regime containing clear rules aimed at improving the detection of suspicious transactions and activities in the crypto ecosystem while protecting consumers and ensuring a level playing field. EFA believes in a risk-based approach that considers the uniqueness of the crypto sector and enables commensurate treatment to ensure that the underpinning technology and CASPs are not disadvantaged with respect to other AML/CFT-obliged entities, products and services.

In particular, we would like to provide comments on the indicated questions below.

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

Amendments to Guideline 8: Sectoral guideline for correspondent relationships

We have concerns with the term 'crypto asset ecosystem' as set out in proposed Guideline 8.6 (d) (iii). This term is overly broad and has the potential to encompass a wide array of participants beyond the intended target, such as all crypto technology providers. As a result, banks may be reluctant to offer services to reputable entities that are not directly involved in CASP activities but are part of the broader technology landscape that supports the crypto asset sector.

We advocate for the following amendment (in bold) to Guideline 8.6 (d) (iii) :

> *'iii. business on behalf of or with **CASPs (or equivalent** providers of services in the crypto-assets ecosystem**)** established in third countries which are not regulated under Regulation (EU) XXXX/XXX9 or under any other relevant EU regulatory framework and which are bound by an AML/CFT regulatory and supervisory regime that is less robust than the regime foreseen in Directive (EU) 2015/849'*

Additionally, in relation to Guideline 8.6 (d) (iv), we disagree with the implication that transactions involving CASPs allowing transfers to and from self-hosted addresses are always associated with higher levels of ML/TF risk.

Transactions executed using self-hosted wallets are securely recorded on the blockchain, a transparent and publicly accessible ledger. Self-hosted wallets empower users with direct control and increase security against the liquidity risks linked to recent exchange failures, significantly contributing to the overall stability and viability of the crypto industry. 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. Self-hosted wallets are privacy-protective but also allow for detection of illicit finance and other harmful activity through transaction monitoring and wallet screening.

The current proposed wording for Guideline 8.6 (d) (iv) carries the risk that banks may refrain from offering banking services to other banks that extend services to CASPs, which subsequently permit transactions to self-hosted addresses. This, in turn, could inadvertently hinder the growth of self-hosted wallets, stifling their adoption and limiting the growth of the crypto ecosystem. The KYC regime already established by the TFR mandates CASPs to perform rigorous due diligence and KYC measures concerning transactions involving self-hosted wallets. These measures are sufficient for CASPs to undertake a comprehensive risk assessment, which will be based on the risks identified in their operations, rather than solely on the utilisation of a self-hosted wallet. As such, we recommend that this line be removed.

Question 7: Do you have any comments on the proposed changes to Guideline 9?

For the same reasons outlined in relation to Guideline 8.6 (d) (iii), we have concerns with the term 'crypto asset ecosystem'.

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

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

Product, services and transaction risk factors

For the same reasons already outlined in relation to Guideline 8.6 (d) (iv), we disagree with the assignment of an inherent higher risk categorization to transactions involving self-hosted addresses as proposed in Guideline 21.3 (d). We recommend that this line be removed.

Additionally, in relation to Guideline 21.3(c), we disagree that products that place no restrictions on the overall volume or value of transactions, contributing to increased risk. We are concerned that this would negatively impact crypto remittance products, as generally CASPs don't put restrictions on the overall volume or value of transactions upfront. Restrictions can be implemented based on the customer profile and history, and assessment of source/destination of funds but, we believe, there shouldn't be restrictions in overall volume or value transactions as a blanket control.

We recommend that this line is removed.

Distribution channel risk factors

In relation to Guideline 21.9 (c), we disagree with the inference that all business relationships between CASPs and their customers that are established through an intermediary service provider in the crypto assets ecosystem outside of the EU, are inherently higher risk. If the bank and CASP have already conducted their own CDD then it should not matter where the business relationship between the CASP and the customer was originally established. We advocate for the removal of this line.

Furthermore, we oppose Guideline 21.9 (e) which infers that any novel distribution channels or new technology used for crypto asset distribution, without prior full testing or usage, should be automatically categorised as high risk. We advocate for a revision of this wording to acknowledge the possibility of increased risk while avoiding a sweeping classification of all new technologies.

We suggest the following amendments (in bold);

'e) new distribution channels or new technology used to distribute crypto assets ~~that has not been fully tested yet or used before~~ ***where the technology or distribution channel introduces elevated levels of ML/TF risk****'*

Enhanced customer due diligence

Furthermore, Guideline 21.12 lists a significant number of measures that CASPs 'must' apply in situations of increased risk, such as obtaining evidence of the source of funds or crypto assets for transactions involving cash/crypto exchanges, crypto asset 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 the requirements set out in the TFR.

We would suggest that the wording reads instead 'Where the risk associated with a business relationship or occasional transaction is increased, CASPs **shall** apply EDD measures pursuant to Article 18 of Directive (EU). In addition, CASPs **may** apply one or all of the following EDD measures'.

Simplified customer due diligence

The provisions outlined in Guideline 21.15 introduce three SDSD measures for CASPs to utilise in low-risk situations which have been classified as such as a result of the ML/TF risk assessment carried out by the CASP in accordance with the EBA's guidelines;

"a) for customers that are subject to a statutory licensing and regulatory regime in the EU or in a third country, verifying identity-based on evidence of the customer being subject to that regime, for example through a search of the regulator's public register;

b) updating CDD information, data or documentation only in case of specific trigger events, such as the customer requesting a new or higher-risk product, or changes in the customer's behaviour or transaction profile that suggest that the risk associated with the relationship is no longer low, while observing any update periods set out in the national legislation.

c) lowering the frequency of transaction monitoring for products involving recurring transactions, like in the case of portfolio management."

We are concerned that these measures disproportionately restrict SDD options for the sector. Notably, none of the proposed options permit more lenient identification or verification standards for individuals, and the reduction in monitoring scope is confined solely to specific products with recurring transactions. This divergence from the approach taken with other financial sectors will create an uneven competitive landscape between crypto-assets and other regulated financial instruments. This approach implies a characterization of crypto-assets even in low-risk scenarios as being inherently more risky than traditional

financial instruments and deviates from the core principles of a risk-based approach. We advocate for a revision of this wording to ensure equitable treatment across all financial sectors.

ABOUT EFA

The European FinTech Association (EFA), the association represents a diverse group of 40 FinTech providers ranging from payments, lending, banking, robo-advice, investment, and software as a service for the finance sector, with a clear focus on enabling a single market for digital financial services.
Digital FinTech companies offering financial services are still subject to scattered regulations and requirements, preventing efficient cross-border growth. Digital financial services can empower all Europeans to manage and maximize their capital, payments, and investments safely and securely.
We believe that tearing down cross-border barriers will ensure that users, regardless of their location, can access the same quality of financial services everywhere. By sharing our deep tech know-how, we foster sound tech regulation that is beneficial for the overall EU financial market, presenting people with the advantages of technology for finance.