28 August 2023

European Banking Authority
Digital Finance Policy Team
Tour Europlaza
20 avenue André Prothin CS 30154
92927 Paris La Défense CEDEX, France

Re: Consultation on the Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849

Dear EBA Team,

Circle is a global financial technology firm that enables businesses of all sizes to harness the power of digital currencies and public blockchains for payments, commerce and financial applications worldwide. Circle is powering always-on internet-native commerce, payments, and custody, and is the issuer of USD Coin (USDC) and Euro Coin (EUROC).

We appreciate the opportunity to provide our comments to the proposal for amending the Risk Factor Guidelines and remain at your disposal for any additional questions you might have.

Question 6: Do you have any comments on the proposed changes to Guideline 8? (Dealing with sectoral guideline for correspondent relationships)

6.1. We recommend using the MiCA-term "crypto-asset service provider" instead of "providers of services in the crypto-assets ecosystem" in Guideline 8.6 paragraph d)(iii). "Providers of services in the crypto-assets ecosystem" is not sufficiently precise to only capture those businesses that would be regulated under MiCA in the EU. For example, it could include providers of technology and ancillary services, such as blockchain analytics, web infrastructure, etc. Such entities are not involved in, and have no control over, the flow of crypto-assets and therefore pose a limited ML/TF risk.

6.2. The proposed amendment in Guideline 8.6 paragraph d)(iv), which provides for factors that indicate a higher risk, proposes that if a respondent conducts "business on behalf of CASPs which allow transfers to and from self-hosted addresses", then this is an indicator of such higher risk. This risk factor would apply to almost all CASPs, thus proposing that correspondents undertaking business with any regulated firm in the crypto asset sector would give rise to high risk.

Self-hosted wallets play an important role in the blockchain ecosystem and have myriad benefits including related to financial inclusion and payment system optionality. According to the FATF, the substantial amount of variation in the data for illicit transactions means that there is currently no consensus on the size of the P2P sector and its associated ML/TF risk.[1]

Furthermore, we believe that with the implementation of the transfer of funds regulation (TFR) to crypto-assets, including requirements for CASPs to mitigate any illicit finance risks when transacting with self-hosted wallets through a risk-based approach (including for example the reception and verification of counterparty data and the use of blockchain analytics tools), any ML/TF risks can be mitigated and limited. As per blockchain analytics, only a small proportion of self-hosted wallets have a high risk profile, which is derived from high risk block-chain activity.

Therefore, generalising the incidence of high risk to all such products is disproportionate and places payment service providers utilising DLT technology at a disadvantage to those adopting a centralised infrastructure, when in fact it is the risk management and risk mitigation that will determine residual risk. This is not technologically neutral and not aligned with the upcoming implementation of the updated TFR, and we therefore suggest deleting this risk factor.

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

7.1. Please see our response 6.1. above in relation to the term “providers of services in the crypto-assets ecosystem” used in Guideline 9.20.

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

9.1. Guideline 21.3 sets out factors that contribute to increasing risk. Paragraph (b) states:
“b) the product allows payments from third parties that are neither associated with the product nor identified upfront, where such payments have no apparent economic sense;”

The scope and meaning of this paragraph is unclear. In what situations are third parties not associated with the product and when would payments not make economic sense? Why would a third party making a payment to a crypto asset wallet be identified by the CASP of the payee? It is of course assumed that the payee CASP will in any event be in receipt of originator travel rule information relating to the payer.

9.2. Guidelines 21.3 (d)(i) sets out factors that contribute to increasing risk; it states:
“d) the product allows transactions between the customer’s account and: i. self-hosted addresses; “

Similarly to our comments made at point 6.2., we disagree that transacting with self-hosted wallets represents in and of itself a higher ML/TF risk. The risk should be balanced against the benefits

[1] FATF second 12 month review of the revised FATF standards on virtual assets and virtual asset service providers, paragraph 6.
https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf.coredownload.pdf

relating to security, privacy and financial inclusion that self-hosted wallets provide, and also against the mitigation measures available and performed under the EU TFR.

9.3. Guideline 21.3 paragraph (d)(ii) sets out factors that increase risk and states the following:

"(ii) crypto-asset accounts or distributed ledger addresses managed by a provider of services in cryptoassets ecosystem which is not regulated under EU law and which is not regulated under any other laws similar to Regulation (EU) XXXX/XXX11, or which is subject to the AML/CFT regulatory and supervisory regime that is less robust than the regime foreseen in Directive (EU) 2015/849."

The aim of this provision is unclear. If these are EU providers that fall outside of the regulatory perimeter of MiCA, the question arises why these are designated as higher risk even though they are not deemed to warrant financial or AML regulation in the EU. If the intention is to capture third country providers, then this should already be captured under Guideline 21.3 paragraph (d)(iii).

9.4. It would be beneficial to add to Guideline 21.4 that transactions between the customer's account and a crypto-asset account or distributed ledger address held by a service provider which is regulated in the EU under MiCA is a factor that decreases risk. Given that both accounts/addresses will be fully verified, and travel rule information will be provided, there is no reason not to regard such transfers between customers of regulated financial institutions as lower risk, particularly given the fact that transactions with third country regulated CASPs are already designated as lower risk in Guideline 21.4 paragraph b(ii).

9.5. Guideline 21.5 paragraph (b)(xv)(b) lists as one of the higher customer risk factors relating to the customer's behaviour where the customer "repeatedly receives crypto-assets from or sends crypto-assets to . . . multiple self-hosted addresses or multiple addresses located in other CASPs."

This provision should be deleted, as without other indicators, the sending and receiving of crypto-assets from/to other wallets can be legitimate behaviour where a crypto-asset product is used for making and receiving payments. The use of multiple addresses is good security practice when pseudonymous transaction information relating to individuals is publicly available on a blockchain and may have additional utilities. The diverse use of counterparties actually allows blockchain analytics services to better profile the counterparty risk. It is not a de facto indicator of risk without additional information.

9.6. Guideline 21.9 paragraph (d) sets out the following distribution channel risk factor, increasing risk:

"d) when commencing a business relationship with a customer, the CASP is using services of an outsourcing service provider in accordance with Article 29 of Directive (EU) 2015/849, to gather CDD from the customer, in particular, where that service provider is located in a high-risk jurisdiction."

The inclusion of the phrase 'in particular' potentially renders the use of any outsourced service provider for CDD a risk factor. Providers in the EU or another low-risk jurisdiction should not be included here.

9.7. Guideline 21.9 paragraph (e) listing factors increasing risk, cites “new distribution channels or new technology used to distribute crypto-assets that has not been fully tested yet or used before” as one of the distribution channel risk factors. This provision should be qualified so that it refers only to those technologies and channels that could give rise to an increased risk of abuse. CASPs are already required to assess the ML/TF risk of any new technology, distribution channel or product innovation as part of their business-wide risk assessment. Where this risk is deemed to be low, the use of such innovations should then not be considered a higher risk factor. It would be disproportionate to provide that all new technologies or distribution channels give rise to increased risk.

9.8. Guideline 21.15 sets out three SDD measures available to CASPs where there is a finding of low risk:

“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.”

This constitutes a severe and disproportionate restriction on SDD measures available to the sector. Of the three measures in paragraphs (a), (b) and (c) there is none that allows for a lower standard of identification or verification of natural persons, and monitoring may only be reduced in the context of specific products that involve recurring transactions.

No other financial sector is restricted in this manner, suggesting an un-level playing field between crypto-assets and other regulated financial instruments. The implication is that even where a situation is found to give rise to a low risk of ML/TF, this still constitutes a higher risk where crypto-assets rather than other financial instruments are involved. This is unwarranted and does not accord with a risk-based approach.

It will specifically discriminate between electronic money tokens (EMTs) under MiCA and electronic money under the electronic money directive which is based on a centralised infrastructure.

We suggest revising the provisions relating to SDD and providing for the benefit of mitigation strategies that could be applied by CASPs and consequently enable them to benefit from a broader application of SDD. This could, for example, address means of verification of identity.

+++

Yours sincerely,

Teana Baker-Taylor
Vice President, Policy & Regulatory Strategy, EMEA

Patrick Hansen
Director, EU Strategy & Policy