Electronic Money Association
68 Square Marie-Louise
Brussels 1000
Belgium
www.e-ma.org

31 August 2023

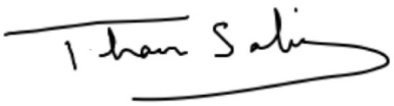
Dear Madam/Sir,

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

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our head office is in Brussels, and we have branches in Ireland, the Netherlands, Luxembourg, Lithuania, and Malta. Our members include leading payments and e-commerce businesses worldwide, providing online payments, card-based products, electronic vouchers, mobile payment instruments and crypto-asset services. Most of our members operate across the EU, most frequently on a cross-border basis. A list of current EMA members can be found here.

We are writing today to respond to your proposal for amending the Risk Factor Guidelines. We hope you will consider our comments and remain available for any questions you might have.

Yours sincerely,



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

EMA response

Question 1: Do you have any comments on the proposed changes to definitions?

We do not have any comments on the proposed changes to definitions.

Question 2: Do you have any comments on the proposed changes to Guideline 1?

We do not have any comments on the proposed changes to Guideline 1.

Question 3: Do you have any comments on the proposed changes to Guideline 2?

We do not have any comments on the proposed changes to Guideline 2.

Question 4: Do you have any comments on the proposed changes to Guideline 4?

We do not have any comments on the proposed changes to Guideline 4.

Question 5: Do you have any comments on the proposed changes to Guideline 6?

We do not have any comments on the proposed changes to Guideline 6.

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

6.1 The use of the term "*providers of services in the crypto-assets ecosystem*" in Guideline 8.6 paragraph d)(iii) is not sufficiently precise to only capture those businesses that would be regulated under MiCA in the EU. It could, for example, 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. We suggest adopting the MiCA term 'crypto-asset service provider.'

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.

Given legitimate and pervasive uses of self-hosted wallets, 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 we therefore suggest deleting this risk factor. Please also see our response at **9.3** below.

6.3 In Guideline 8.6, a new provision indicating higher risk has been added at paragraph h), it states:

"*h) the ownership of the IBAN account provided by a respondent CASP to receive fiat funds from customers is in the name of a company other than the CASP.*"

This risk factor could include IBANs accounts owned by a group company of the respondent CASP, which does not warrant the higher-risk designation. It is also normal practice to for CASPs to partner with banks or EMIs for the provision of fiat on/off ramp functionality, and it should be made clear that this is not what this risk factor aims at.

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

7.1 Please see our response at paragraph **6.1** above in relation to the term "providers of services in the crypto-assets ecosystem" used in Guideline 9.20.

7.2 In order to account for effective AML/CTF regulatory regimes applicable to crypto-asset service providers in third countries, paragraph 9.20 should be amended to add the following phrase: '***and which are bound by an AML/CTF regulatory and supervisory regime that is less robust than the regime foreseen in Directive (EU) 2015/949***' after "*any other relevant EU regulatory framework*." This would better calibrate the risk assessment process undertaken by banks who are the subject of this provision.

We also make the same comment as we did at Guideline 8.6 (d)(iii) in relation to the inclusion of the word 'ecosystem' which brings in a range of service providers that have little or no relevance in relation to the crypto-asset service providers themselves.

7.3 In view of our comment at **7.2** above, paragraph d) in Guideline 9.21 could be deleted.

Question 8: Do you have any comments on the proposed changes to Guidelines 10, 15 and 17?

8.1 In its current form, Guideline 17.4 paragraph (i) would discriminate against crypto-asset forms of payment, which cannot be appropriate given the objectives of both AML and prudential (MiCA) regulation. We suggest qualifying the text to indicate such distinction only when anonymising features for example are employed.

8.2 Our comments in relation to paragraph 8.1 equally apply to Guideline 17.6 paragraph (b).

<u>Guideline 21: Sectoral guideline for crypto asset services providers (CASPs)</u>

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 are 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 Paragraph 21.3 (c) states:

"c) the product places no restrictions on the overall volume or value of transactions;"

On its own, the absence of volume/value restrictions associated with a product does not constitute a higher risk; it would also apply to most cryptoasset products. The product aspect that is significant in terms of risk is whether the higher risk associated with a higher volume/value going through an account is mitigated appropriately by means such as transaction monitoring, red flagging, manual checks, temporary restrictions, etc. We therefore suggest amending this risk factor to say 'c) the product places no restrictions on the overall volume or value of transactions ***in the absence of appropriate risk mitigating controls in cases of increased transactional activity***.'

9.3 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; "

Our comments at paragraph **6.2** addressing the attribution of high risk to self-hosted wallets are relevant under this paragraph; self-hosted wallets are a means for users to administer their private keys and has benefits relating to security, privacy and resilience. The risk posed by the use of self-hosted wallets must be balanced against the benefits that they provide, as well as the mitigation strategies available. It is not helpful to classify the product as giving rise to increased or high risk without qualification, as this might lead to de-risking of the DeFi sector.

Data on the risks of unhosted wallets remains incomplete, as is recognised by the FATF's *Second 12-Month Review of The Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers*, which states that "the substantial amount of variation in the data means that there is no consensus on the size of the P2P sector and its associated ML/TF risk (p. 3)." Accordingly, the FATF's *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* encourages jurisdictions "to assess and monitor the risks associated with unhosted wallets, including P2P transactions, and share their experiences, including on data collection and risk assessment methodologies and findings, as well as practice in mitigating risks (p. 5)." In the absence of appropriate data, a cautious approach should be taken to classifying unhosted wallets as higher risk.

It should also be noted that the transfers listed in Guideline 21.3 (d) are subject to travel rule requirements that already mitigate the risk of ML/TF. Where the travel rule is complied with, transfers of this kind do not warrant being classed as higher risk. We therefore suggest adding to the end of paragraph (d) '***where the travel rule requirements could not or could only incompletely be complied with, whether due to issues with wallet attribution or otherwise***.'

9.4 Reference is made in a number of provisions to the "*crypto asset ecosystem*". We have addressed the difficulties associated with this in our response at paragraph **6.1** above. It is again used in Guideline 21.3 paragraph (d)(ii) and (iii), Guideline 21.4 paragraph (b)(ii), Guideline 21.6 paragraph (d), Guideline 21.8 paragraph (a) and Guideline 21.9 paragraph (c). We make the same comments as to the overly broad meaning of ecosystem and that it will capture far more than would be proportionate under the Guidelines.

9.5 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 crypto-assets ecosystem which is not regulated under EU law and which is not regulated under any other laws similar to Regulation (EU) XXXX/XXX[11], 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 permitter 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 is should already be captured under Guideline 21.3 paragraph (d)(iii).

9.6 The designation of transfers from e-money instruments exempted from CDD under Article 12 4MLD is disproportionate. This is because such e-money instruments have already been overly restricted in their scope, to a maximum online transaction value of EUR 50 and a maximum monthly transaction limit of EUR 150. It is impossible to see how this gives rise to any 'high' or 'higher' risk in any context. Furthermore, transfers of e-money issued outside the EU regulatory and supervisory regime should only be designated as a higher risk factor if the issuer is subject to a less robust AML regime.

9.7 Guideline 21.3 paragraph (f) indicates increased risk associated with:

"f) where the CASP is offering nested services (a service within a service) of a wholesale CASP where the wholesale CASP exercises only weak control over the nested service."

This risk factor would benefit from clarification, as it is not clear what scenario is aimed at here.

9.8 Guideline 21.4 sets out factors that reduce risk. In order to mirror Guideline 21.3 on factors that increase risk, Guideline 21.4 paragraph (b)(ii) should say '. . . which is regulated outside the EU under the regulatory framework, that is as robust as that foreseen in Regulation (EU) XXXX/XXX13 ~~and~~ ***or*** which is subject to AML/CTF regulatory and supervisory framework that is as robust as the one provided for in Directive (EU) 2015/849.'

9.9 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).

Another factor reducing risk that could usefully be added here is the use of blockchain analytics to assess and categorise the risk of transactions.

9.10 Guideline 21.5 addresses customer risk factors, organising these as factors relating to the 'nature' of the customer and factors relating to the customer's behaviour. Guideline 21.5 paragraph (a)(v) states:

v. an undertaking, which is in an intra-group relationship with other crypto-asset businesses;

This risk factor would benefit from clarification, as it is not clear what scenario is aimed at here. Drafted as it is, the wording might include a broad range of business setups between regulated entities. Therefore, we suggest at least including '***where both entities in the intra-group relationship are not regulated***.'

9.11 In relation to Guideline 21.5 (b)(xi)(e), please refer to our comments regarding anonymous e-money instruments that are exempted from CDD under Article 12 4MLD, set out at paragraph 9.6 above. These are overly restricted and cannot be regarded as giving rise to any increase in risk. They are certainly not comparable to cash, while privacy coins could be a broad class of instruments with varying attributes.

9.12 Guideline 21.5 paragraph (b)(xiii) describes customer behaviour that should be regarded as increasing risk, stating that the customer "*directly or indirectly receives or sends crypto assets related ML/TF or related criminal activities previously identified as such.*"

This risk factor should be qualified to avoid tokens that have been cleared of their association with criminal activities (for example, after being confiscated and auctioned off by law enforcement) being caught. This will be apparent from the risk grading applied by blockchain analytics. The impression that entire classes of cryptoassets (such as Bitcoin) are aimed at here should also be avoided. We suggest the following amendments: 'directly or indirectly receives or sends crypto asset~~s~~ ***tokens*** related ***to*** ML/TF or related ***to*** criminal activities previously identified as such ***and which continue to be identified as such***.'

9.13 Guideline 21.5 paragraph (b)(xv)(a) suggests a higher risk associated with a customer where that customer repeatedly receives/sends crypto-assets through an unregulated or lesser regulated intermediary. However, the use of specific intermediaries is neither determined nor under the control of customers. Furthermore, as long as intermediaries comply with the travel rule requirements

applicable in the EU and the CASP complies with its CDD obligations in relation to the customer, the ML/TF risk should not be seen as heightened simply because an intermediary involved is not in scope of regulation or subject to a less robust AML regime in the jurisdiction in which it is based.

9.14 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 transaction information relating to individuals is publicly available on a blockchain and may have addition utilities. It is not a de facto indicator of risk.

9.15 We suggest adding a customer factor decreasing risk to the list in Guideline 21.6, namely, exchanges of crypto assets where either the source or destination for the crypto asset is a crypto asset account or distributed ledger address held by a service provider which is regulated in the EU under MiCA (please also see our comment at paragraph **9.9** above).

9.16 Guideline 21.6 paragraph (e) lists the following as a factor reducing customer risk:

"e) [the customer] requests an exchange and either the source of or destination for the crypto asset relates to low value payments for goods and services to/ from a lawful merchants or service providers."

The reference to 'lawful' merchants and service providers in this provision should be deleted, as CASPs that are exchanging crypto-assets will not have a customer relationship with such merchants and service providers are therefore unable to assess their lawfulness.

9.17 Guidelines 21.7 paragraph (d) and 21.8 paragraph (a) incorporate the level of predicate offences in a jurisdiction into higher (21.7 paragraph (d)) and lower (21.8 paragraph (a)) country or geographical risk factors:

"21.7 d) The business relationship is established through the CASPs or crypto-ATMs, which are located in regions or jurisdictions outside the EU and are associated with high levels of predicate offences or the risk of ML/TF.

21.8 a) where the transfer comes from or is sent to a crypto asset account or a distributed ledger address that is hosted by a provider of services in crypto assets ecosystem that is regulated and supervised outside the EU under a regulatory framework that is as robust as the one foreseen in Directive (EU) 2015/849 and that foreseen in Regulation (EU) XXXX/XXX19 and which is as- sociated with low levels of predicate offences."

This has a disproportionately negative effect. The level of predicate offences in jurisdictions that have an effective AML regime does not have a direct connection to the risk of ML/TF taking place. This is because the nature of predicate offences differs across jurisdictions; a country with an 'all crimes approach' to predicate offences, could therefore find itself having a high level of offences (all crimes being counted) compared to another with a 'serious crimes' approach (only serious crimes being

counted). It would be better to refrain from reference to predicate offences and to address ML/TF risk.

9.18 Guideline 21.9 paragraph (b) lists as one of the distribution channel risk factors that increase risk:

"b) there are no restrictions on the funding instrument, for example in the case of cash, cheques or electronic money products, that benefit from the exemption under Article 12 of Directive (EU) 2015/849."

The reference in this provision to e-money that is exempted under Article 12 4MLD is misinformed, given the highly-restricted nature of e-money instruments that qualify for this exemption. Also see our response at paragraphs **9.6** and **9.11** above.

9.19 Guideline 21.9 paragraph (c) lists a distribution channel risk factor that increases risk as:

"c) the business relationship between the CASP and the customer is established through an intermediary service provider in crypto assets ecosystem outside the EU, which is unregulated or is subject to AML/CTF regulatory and supervisory framework that is less robust than the one provided for in Directive (EU) 2015/849."

Please see our comment at paragraph **9.13** above, which equally applies here.

9.20 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.

There is also some uncertainty as to whether the generalisation that is made in relation to outsourced service providers established in high-risk jurisdictions is better qualified. It may otherwise be inconsistent with the outcome of obligations for firms to oversee such outsourced service providers, including compliance with EBA Guidelines in relation to outsourcing.

9.21 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 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.

9.22 Guideline 21.12 paragraphs (a)-(l) list a significant number of measures that CASPs must apply in situations of increased risk, seemingly in addition to EDD measures under Article 18 4MLD, and these then appear also to be required cumulatively. Is this the intention? If it is, this is highly disproportionate given that risks will already be mitigated, and travel rule requirements complied with. We suggest the following amendment: 'Where the risk associated with a business relationship or occasional transaction is increased, CASPs must apply EDD measures pursuant to Article 18 of Directive (EU) 2015/849 as set out in Title I. ~~In addition,~~ ***Where appropriate,*** CASPs ~~should~~ ***could also*** apply ***one or all of*** the following ***additional*** EDD measures:'

The evidence requirements in paragraph d) are particularly onerous and may lead to the closing of accounts where such evidence cannot be obtained or appropriately verified. Consideration should also be given to future-proofing the guidance. Staking rewards, for instance, are becoming more prevalent and do not warrant inclusion here.

9.23 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 and its timing.

List of EMA members August 2023

AAVE LIMITED
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
Amazon
American Express
ArcaPay UAB
Banked
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network EMEA Limited
Boku Inc
Booking Holdings Financial Services International Limited
BVNK
CashFlows
Checkout Ltd
Circle
Citadel Commerce UK Ltd
Contis
Corner Banca SA
Crypto.com
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
emerchantpay Group Ltd
Etsy Ireland UC
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
J. P. Morgan Mobility Payments Solutions S. A.
Modulr Finance Limited
MONAVATE
MONETLEY LTD
Moneyhub Financial Technology Ltd
Moorwand
MuchBetter
myPOS Payments Ltd
Nuvei Financial Services Ltd
OFX
OKG Payment Services Ltd
OKTO
One Money Mail Ltd
OpenPayd
Own.Solutions
Park Card Services Limited
Paymentsense Limited
Paynt
Payoneer Europe Limited
PayPal Europe Ltd
Paysafe Group
Paysend EU DAC
Plaid
PPRO Financial Ltd
PPS
Ramp Swaps Ltd
Remitly
Revolut

Ripple
Securiclick Limited
Segpay
Skrill Limited
Soldo Financial Services Ireland DAC
Square
Stripe
SumUp Limited
Swile Payment
Syspay Ltd
Transact Payments Limited
TransferMate Global Payments
TrueLayer Limited
Trustly Group AB
Uber BV
VallettaPay
Vitesse PSP Ltd
Viva Payments SA
Weavr Limited
WEX Europe UK Limited
Wise
WorldFirst
Worldpay
Yapily Ltd