European Crypto Initiative

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

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

31 August 2023

EUCI

Question 1:

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

We call for consistency across different regulations, which is key to ensuring the same interpretation of the provisions by all addressees and enables easier implementation of the guidelines in business operations without the need for adaptation or translation of individual terms, thus avoiding confusion and enforcement errors. Therefore, we understand the need to unify the definitions and have no particular objections towards this approach.

Nevertheless, we call for the postponement of the suggested terminology unification, as the meaning of the used term is dependent upon the final texts of both the upcoming Anti-Money Laundering Regulation and the updated version of the AML Directive. A clear example of the ongoing activities related to defining the scope of "financial institutions" can be observed in Recital (59) from the Transfer of Funds Regulation, which calls for the inclusion of CASPs into the broader category of "financial institutions," as defined in the current version of the AMLD.

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

However, the AMLD is currently undergoing regulatory revision, with the definition of "financial institutions" likely to become part of the proposed AML Regulation (see Article 2 (6) of the Proposal for the AMLR). Furthermore, according to the Proposal for the AMLR, CASPs would fall under the broader category of "natural or legal persons acting in the exercise of their professional activities" (Article 3, (3) g) of the Proposal for the AMLR). Therefore, we would ask for the delay of revisiting the scope of these Guidelines until there is certainty around the categorisation of CASPs and their potential inclusion into the broader scope of "financial institutions".

If any such delay in adopting the revised Risk Guidelines proves not to be possible, in order to avoid confusion, we suggest refraining from using the words CASPs and firms separately as "firm" should automatically apply to CASP as well, unless, when for example, CASP is excluded.

Furthermore, we also suggest the following addition to the definitions provided in the Risk Guidelines, as it would better represent the practical reality of non-face to face relationships or transactions:

> f)'Non-face to face relationships or transactions' means any transaction or relationship where the customer is not physically present, that is, in the same physical location as the firm or a person acting on the firm's behalf. This includes situations where the customer's identity is being verified via video-link, **liveness checking**, or similar technological means.
>
> h) The definition of "Pooling bank account" is also to be amended to include "omnibus account" in order to administer fiat deposits that belong to the customer's own clients.

Question 2:

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

EUCI considers the "Keeping risk assessments up to date" category of Guideline 1 to be very well thought out and to set a good system in place. However, the proposed additional *point d*. introduces potentially unachievable requirements for CASPs in particular, as it sets a requirement for risk assessments for activities that might be understood very broadly in the context of crypto asset activities.

For example, while the introduction of new delivery mechanisms for traditional financial institutions might be an activity requiring months of planning and careful technical assessment - for example, a bank opening a new physical branch or the introduction of a mobile application - CASPs' services usually don't use intermediaries and physical delivery mechanisms and, therefore, do not pose the same risks regarding the adoption of new delivery mechanisms.

Furthermore, due to the direct nature of crypto services, it is likely that a wide range of low-risk CASP activities would fall into the category of "delivery mechanisms", leading to potential confusion and

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

overburdening due to the need for a disproportionate number of high-risk assessments in comparison to the riskiness of the activities.

Therefore, more clarity needs to be provided regarding what "delivery mechanism" means in the context of CASPs' activities. If the delivery mechanism stands for a sales channel, we suggest this to be clarified. An explanation of what is considered a "delivery mechanism" would ensure more effective and easier implementation of the guideline.

We suggest the following wording to be added to *point d.*: 'Where the firm is launching a new product or service, or a new business practice, including a new delivery mechanism **which significantly impacts the delivery of the service**, or is adopting an innovative technology as part of its AML/CFT systems and controls framework, it should assess the ML/TF risk exposure prior to the launch and reflect this assessment in the firm's business-wide risk assessment and its policies and procedures.'

With regards to Guideline 1.7. a) We suggest the requirement be changed in the direction that the firm needs to perform business-wide risk assessment updates on planned intervals, a minimum of once per calendar year. This would force firms to consider whether the risk assessment update needs to be performed bi-yearly or in certain parts, even in shorter periods.

We suggest the following amendment to Guideline 1.7. a) "Setting dates on planned intervals for each calendar year considering the internal and external issues that are relevant to the firm's business, however on a minimum yearly basis, by setting (a) date(s) on which the next business-wide risk assessment update will take place, and setting a date on a risk sensitive basis for the individual risk assessment to ensure new or emerging risks are included".

Question 3:

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

We generally agree with the need for extra caution when CASPs' professional activities involve ensuring that neither customers nor beneficial owners have links to unregulated businesses that provide services related to crypto assets.

Nevertheless, it is likely that the purpose of Guidance 2.4. will be clearer and would, therefore, be served better if it refers to Guideline 9.20 instead of Guideline 9.21.

Therefore, we propose the following change to *point b.*:

'Does the customer or beneficial owner have links to sectors that are associated with higher ML/TF risk, for example certain Money Service Businesses, unregulated businesses that provide services related to crypto assets as described in Guideline 9.20, casinos or dealers in precious metals?'

European Crypto Initiative

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

Question 4:

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

Regarding *Guideline 4.29*:

We agree with the need for relevant and adequate measures in place regarding remote customer onboarding. Nevertheless, the current wording of Guideline 4.29 might potentially lead to uncertainties regarding the applicability of the Guidelines on the use of Remote Customer Onboarding Solutions to CASPs and whether CASPs will only need to apply the measures listed under Guideline 4.29 a) and b) or would the whole Guidelines on the use of Remote Customer Onboarding Solutions be applicable also to CASPs. For this reason, we suggest that an additional clarification be included, according to which only measures under Guideline 4.29 apply to CASPs (and not the whole Guidelines on Remore Customer Onboarding Solutions).

In addition, we consider that the non-face-to-face nature of the relationship automatically poses ML/TF risk, thus the firm needs to ensure the solution for remote identification is reliable, thus 4.29 c) seems partially redundant, and we suggest that it be amended in the following way: “assess whether the non-face to face nature of the relationship in conjunction with occasional transactions gives rise to increased ML/TF risk and if so, adjust their CDD measures accordingly. When assessing the risk associated with non-face-to-face relationships, firms should have regard to the risk factors set out in Guideline 2.”

Regarding *Guideline 4.35*:

We consider this addition to be reasonable, as timely access to information is oftentimes a requirement for the running of normal day-to-day business operations. Nevertheless, this prompt access should not come at the price of data protection and should still be done in accordance with the applicable data protection regulations.

The data transfer and retention in case of termination of the relationship with the external provider is to be considered as well, namely, the service agreement with the external provider should entail clauses for data management in case of termination of the agreement, in particular, to assure data transmission is provided in a form that ensures integrity and uninterrupted accessibility.

Regarding *Guideline 4.60*:

We understand and support the need to implement FATF recommendations within the updated risk guidelines. Furthermore, we suggest the following text to be added to Guideline 4.60: d) “the transactions differ from the transactions either in the amount or frequency or complexity or similar as stated by the customer during the onboarding procedure.”

Regarding *Guideline 4.74*:

We agree with the proposed wording of *point d*, as it leaves enough space for a case-by-case implementation and for the development of a healthy and competitive market for DLT analytics tools.

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

However, it is worth noting that since analytical blockchain monitoring is not possible without technical tools, and considering the authorities require the CASPs to have such tools in place, the question is more for the CASPs to decide which tools to use appropriate to the needs of their business, and not if to be used.

In addition, we suggest also considering the inclusion of AI solutions. This can serve as a reference for companies to stay atop the latest industry developments.

Question 5:

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

We agree with the proposed additions to Guideline 6 as conducting the proposed types of staff training will likely greatly enhance the risk avoidance capabilities of the CASP.

However, we propose the following addition to Guideline 6.2. In order to enhance clarity:

6.2. As part of this, and in line with the guidance contained in Title I, firms should take steps to ensure that staff, **in the scope of their position and responsibilities,** understand [...]

Question 6:

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

Regarding Guideline 8.6:

We would like to ask for more clarity regarding the following issues with the proposed text of Guideline 8.6:

- How would one determine which AML/CFT regulatory and supervisory regimes are to be considered as robust as the regime, foreseen in Directive (EU) 2015/849? Would, for example, following FATF's recommendations be a necessary aspect of this evaluation?
- With regards to Guidance 8.6.b - The respondent is not subject to adequate AML/CFT supervision. How will this be evaluated? To avoid subjectivity and enforcement of obligations where the expectations for fulfilment are not clear we suggest the public resources in the countries with indications of a higher ratio of corruption and other exposure are to be taken into consideration.
- Furthermore, we consider that Guidance 8.6.d) iv. needs more clarity in which case such risk is considered to be increased, namely in a practical sense to be explained what business model is targeted by this. If such an explanation is not possible, we ask for the deletion of Guidance 8.6. d) iv.

Our reasoning is that it is not unusual for CASPs to allow transfers to and from self-hosted addresses as this activity does not necessarily relate to risk indicators. Using self-hosted addresses is a usual practice. Self-hosted wallets are one of the biggest advantages of blockchain technology, making any general consideration that they indicate higher risk not accurate. The self-hosted wallet is considered risk-related when blockchain analytical tool indicates certain relations to fraudulent transactions. So instead of the

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

general assumption that they are risk-related, we suggest amending with requirement only to cases when a blockchain analytical tool indicated an exposure to risk.

- Further, we consider the risk, described in Guidance 8.6.d v) about businesses with non-residents also redundant, as clients coming from a selection of countries in which higher ML/FT is indicated, are in any case considered to relate to higher risk. The mere non-residency within the EU should not automatically represent a higher risk. Therefore, we ask for the deletion of Guidance 8.6.d v).
- Furthermore, the risk indicator under Guidance 8.6.d vi) business in a currency other than that of the country in which it is based should also per our opinion, not represent an automatic trigger for higher risk, namely cross border provision of services has more success if supported by local currency, so this risk is to be interpreted together with business model. Therefore, we ask for the deletion of Guidance 8.6.d vi).

Regarding Guideline 8.8:

We would like to ask that more clarity is provided regarding the proposed text of Guideline 8.8, particularly in relation to what would constitute a “sufficient level of certainty” in this context of that Guideline and the practical aspects of its establishment.

Furthermore, we also consider the requirement under Guideline 8.8. d) to be redundant - first checking if the client is based in a jurisdiction associated with higher ML/TF risk, and if not, additional verification is needed if this assumption is correct. The checking whether the client is in ML/TF jurisdiction should be based on a method that is considered sufficiently certain - thus, we consider Guideline 8.8 d) is not needed and needs to be deleted.

- Further, what level of attempt at verifying an IP address would sufficiently meet the requirements of the proposed Guidance?
- What public resources should be used to identify countries with significant levels of corruption and/or other predicate offences to money laundering, without the adequate capacity of the legal and judicial system effectively to prosecute those offences, with significant levels of terrorist financing or terrorist activities; or without effective AML/CFT supervision.

Regarding Guideline 8.17:

Measures related to respondents based in a non-EEA country should be adjusted to the jurisdiction of the respondent and evaluation of the risk related to that particular entity, and not represent such a burden and overhead that the financial institution would rather simply not accept any such clients as they will deduct there is too much work and resource needed that does not justify entering into relationship with non-EEA client. As a general note, we suggest the listed measures to be applied by taking into consideration the respondent business, complexity, volume of the transactions, and similar.

Furthermore, as also expressed in the answer to Question 1, we consider this not to be the right moment for revisiting the Risk Guidelines due to their dependency on EU regulations that are currently undergoing

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

significant changes (relevant in this case - the AML Directive), as well as due to the ongoing work on a new AML Regulation that has the potential to reshape the EU policies towards combatting money laundering significantly. Therefore, we ask for the postponement of the work done towards redrafting the Risk Guidelines after the finalisation of the remaining files from the AML package.

Question 7:

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

Regarding the proposed Guideline 9, we would like to make a general remark by emphasising that banks should still be clearly encouraged to cooperate with CASPS and not simply ban clients that fall into the CASP category (unfortunately, a practice that is often seen on the market). With only a few banks supportive towards the crypto industry, this represents a major obstacle to further industry development as well as further market adoption. In addition, the expenses that a CASP is required to pay for opening a bank account and for the onboarding process are, in most cases, much higher than compared with other industries.

The most common reasons/arguments for not enabling bank accounts to CASPs are that banks do not have sufficient resources and that requirements for handling such clients are too complex and are considered too risky. With the support of EBA, we hope for the reconsideration of this stance and for a change in the practices of banks, which should become more open to cooperating with CASP, preferably declining the cooperation solely on an argumentative basis, which is not based only on arguments about cost and lack of resources.

Furthermore, MiCA will bring harmonisation and requirements comparable with the financial institution regime, leading to banks having no more reasons to decline CASPs as customers automatically.

We would like to ask EBA for increased vigilance towards finding a solution to these discriminative practices.

Regarding Guideline 9.16:

In reality, banks usually don’t possess information about clients with omnibus accounts. Furthermore, we would like to stress that the requirement for full CDD measures, including treating the customer’s clients as the beneficial owners of funds held in the pooled account and verifying their identities, is not viable. Therefore, we consider that Guideline 9.16 should be deleted entirely.

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

This is due to the fact that the bank should ensure the CASP is providing KYC and EDD, but there is no practical reason for the transfer of such data to the banks. For example, a CASP may have thousands of clients depositing to its pooling account, and disclosing information for each client and applying full CDD measures, including measures for beneficial owners, does not make sense, nor do we see justification for such disclosing of personal data, specifically as CASPs are required to provide such measures.

Furthermore, such a requirement is impossible to fulfill in practice, turning it into an obstacle and a potential excuse for banks not to cooperate with CASPs, in this case also justifiably, since this would entail an enormous amount of extra work regarding individuals that are not even the bank's clients.

Providing such information to the banks would also negatively affect the adoption in the market, as clients' personal data would be shared with banks without their control.

Regarding Guideline 9.20:

We suggest clarifying what is meant by "banks should also consider the ML/TF risk associated with the specific type of crypto assets," namely when this requirement is expected to be followed, e.g. would it be followed in the case of ICOs, or would that be a general rule.

We emphasise this so that banks will be able to understand the requirement and implement it when needed easily.

Therefore, we suggest the following edits to the proposed Guideline 9.20: When entering into a business relationship with a customer who is a provider of **crypto asset services** established in a third country, which is not regulated under Regulation (EU) [xxxx/xxx]10, or **is established within EU but is not regulated** under any other relevant EU regulatory framework, banks may be exposed to increased risk of ML/TF. Banks should carry out the ML/TF risk assessment of these customers and, as part of this, banks should also consider the ML/TF risk associated with the specific type of crypto assets.

Question 8:

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

We strongly support the need for consistency across different regulations, which is key to avoiding confusion and enforcement errors. Therefore, we understand the need to unify the terminology used across the whole spectrum of EU publications and have no particular objections towards this approach and its implementation as part of Guidelines 10, 15 and 17.

Question 9:

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

European Crypto Initiative

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

Regarding guideline: 21.1.

We would like to point out the importance of delineating between the different categories of privacy-enhancing tools and distinguishing between the level of risk they pose. While it is true that the use of certain categories of the so-called "privacy tools" poses a significant money laundering risk, this risk is far from the norm, as most of those tools enhance the overall level of trust and security of the system. In order to better explain the above, EUCI has worked on a brief document that provides an overview of the current state of development of privacy-enhancing tools and their level of risk (it can be found as an attachment to this response). Therefore, we would ask for a more granular approach when determining the risk level of privacy-enhancing tools by abstaining from general rules but instead focusing on a case-by-case approach.

Furthermore, as previously highlighted above, we consider it better to revisit the Risk Guidelines once all files from the AML Package have been finalised due to the significant role that the upcoming AML Regulation will likely have on the use of privacy tools.

Regarding guideline 21.3

21.3. The following factors may contribute to increasing risk:

a) the products or services offered by CASPs entail privacy-enhancing features or offer a higher degree of anonymity such as, but not limited to, mixers or tumblers, obfuscated ledger technology, Internet Protocol (IP) anonymizers, ring signatures, stealth addresses, ring confidential transactions, atomic swaps, non-interactive zero-knowledge proofs and so-called privacy coins;

While we agree that the so-called privacy-enhancing tools of features might oftentimes lead to higher ML/FT risk, it is still crucial to keep in mind that those tools are not the same and have a varying level of individual risk, which needs to be evaluated on a case by case basis. We have prepared an overview of some of the most common privacy tools available that we hope can serve as guidance of that said risk spectrum (provided as an attachment to this submission).

Furthermore, as already stated in answers to previous questions from this consultation, it is crucial that the updated Risk Guidelines are aligned with the final versions of all the files from the AML Package and it is therefore advisable to postpone the redrafting process of the Guidelines for after the AML Directive and the AML Regulation, in particular, have been finalised.

b) the product places no restrictions on the overall volume or value of transactions.

We suggest the following amendment: "The product places no restrictions **or EDD measures** on the overall volume or value of transactions."

a) the product allows transactions between the customer's account and:

    i. self-hosted addresses;

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

We suggest this to be amended so that includes a requirement of a blockchain analytical tool indicating risk exposure to that particular address - see also our answer to Question 6 above.

> 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/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

As stated as part of answers, provided above, we would like to ask for further clarifications regarding the requirement of evaluating the robustness of the AML/CFT regime, as well as to provide the following changes to the text of this Guideline:

> crypto-asset accounts or distributed ledger addresses managed by a provider of **crypto-asset services** which is not regulated under EU law and which **is established within EU but is not regulated** under any other laws similar to Regulation (EU) XXXX/XXX11

> iii. crypto-asset accounts or distributed ledger addresses managed by a provider of services in a crypto-assets ecosystem established in a third country, which is not regulated under Regulation (EU)XXXX/XXX12 or under any other EU relevant regulatory framework, and which is subject to the AML/CFT regulatory and supervisory regime that is less robust than the regime foreseen in Directive (EU) 2015/849

We would like to ask for the deletion of Guideline 21.3. c) iii, due to its duplication with Guideline 9.20.

> iv. a peer-to-peer cryptocurrency exchange platform or a mixer or a tumbler platform;

We suggest the following changes based on the difference of the risk profile both within the broader bategory of peer-to-peer crypto-asset exchanges and between peer-to-peer crypto-asset exchanges and mixer or tumblers (for the latter, please see the attached overview of privacy tools):

a **high-risk** peer-to-peer crypto-asset exchange platform.

> v. crypto-assets' decentralized or distributed application, which is not controlled or influenced by a legal or natural person (often referred to as 'decentralised finance' (DeFi));

We are particularly concerned regarding the proposal for Guideline 21.3. v. due to the following:

1. The low level of risk posed by using DeFi applications, as well as
2. The possibility of creating a dual supervisory regime towards DeFi in the EU.

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

From the literature review (e.g. FATF's V*irtual Assets: Targeted Update on Implementation of the FATF Standards from June 2023* and the US Department of Treasury's DeFi Risk Review), it is apparent that most of the DeFi risks cited there are related to vulnerabilities of the infrastructure rather than the money laundering risks posed by its use. Furthermore, currently, there does not seem to be any comprehensive risk assessments that lead to the conclusion that the users of DeFi services should be considered as posing a higher risk in comparison to the users of traditional financial services or crypto-asset services.

Furthermore, many of the quoted surveys by FATF are indicating progress in mitigating DeFi risk rather than an increase in the concerns.

We are also concerned about the ease with which the term "DeFi" is often attributed to projects that have clear and intended centralised control. We do not argue that such entities should be regulated and the risk they pose should be mitigated. However, such centralised entities should fall within the scope of CASPs/VASPs and should not be a basis for concern regarding the evaluation of DeFi risk.

Therefore, we consider that more legal certainty is required as to what is meant by "DeFi" before such assessments are made, as they risk creating unnecessary burdens for users, CASPs and financial and credit institutions alike that are not related to the specific level of risk, posed by the DeFi application.

Furthermore, another concern we would like to express is that of creating a duplicate legal regime regarding DeFi due to its current exclusion from the scope of MiCA. By including DeFi in the Risk Guidelines, there is a real risk of having different definitions of DeFi used in different circumstances - one for AML risk evaluation and one regarding the rules for CASPs. This would lead to uncertainty, complexity and even unintended illegal behaviour.

Apart from the effect on private entities, this legislative duplication will lead to the potential duplication of competent authorities, with AML authorities and the competent authorities under MiCA likely coming to a different conclusion when evaluating the decentralised nature of a project for the purposes of authorisation under MiCA and AML risk assessment.

> vi. crypto-ATMs or other hardware that involves the use of cash or electronic money, that benefits from exemptions under Article 12 of Directive (EU) 2015/849 or that does not fall within the regulatory and supervisory regime in the EU.

We would like to ask for further details as of what is meant by "other hardware" in this context, as this formulation creates an unnecessary wide scope of potential hardware devices, falling within this Guideline.

a) products involving new business practices, including new delivery mechanisms, and the use of technologies where the level of the ML/TF risk is not yet fully understood by the CASP;

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

As also stated in answer to Question 2 above, more clarity needs to be provided regarding what "delivery mechanism" means in the context of CASPs' activities. If the delivery mechanism stands for a sales channel, we suggest this to be clarified. An explanation of what is considered a "delivery mechanism" would ensure more effective and easier implementation of the guideline.

Furthermore, more information is needed regarding the intended meaning of "ML/TF risk, not yet fully understood by the CASP".

Regarding guideline 21.5,

As a general note, many of the risk factors may pose a risk or not, depending on other circumstances or a combination of different factors. Thus, we suggest adding that all these factors need to be applied on a case-by-case basis, considering the business and internal assessment of the risk factors.

Furthermore, we have the following questions for further clarification and specific proposals for edits to the proposed Risk Guidelines:

a) regarding the **nature of the customer** in particular:

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

We suggest further clarifying in what sense it is considered as higher risk.

b) regarding the **customer's behaviour,** situations where the customer

V. appears to belong to a group of individuals that conduct their transactions at single or multiple outlet or locations or across multiple services;

We suggest amending with an explanation of what is meant by "appears to belong to a group of individuals that conduct their transactions at single or multiple outlet or locations or across multiple services".

VII. appears to persistently avoid CDD requirements by transferring amounts of crypto assets that are just below the threshold defined in Article 14(5) and Article 16(2) of Regulation (EU) 2015/847 (recast);

We suggest the following addition to the Guideline, in order to avoid the risk of ordinary transactions being

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

flagged as high-risk:

appears to persistently avoid CDD requirements by **frequently** transferring **unordinary** amounts of crypto assets that are just below the threshold defined in Article 14(5) and Article 16(2) of Regulation (EU) 2015/847 (recast);

VIII. indicates that the purpose is to invest in an ICO or in a crypto as set/product offering a high return or to invest in a crypto asset which is not supported by a white paper required under the Regulation (EU) xxxx/xxx.

An investment in an ICO or product offering a high return is not necessarily correlated with an increased risk of money laundering, but rather is rather correlated to the risk appetite of the client. We suggest amending this Guideline in the following way:

indicates that the purpose is to invest in an ICO or in crypto as set/product offering **with high fraud-related indications and** a **disproportionately** high return.

XI. uses multiple bank or payment accounts, credit cards or prepaid cards to fund the crypto assets account;

We would like to emphasise that the number of credit cards does not reflect the risk itself, as many users use disposable credit cards to increase the safety of their online shopping.

XV. is investing or exchanging crypto assets, which it has borrowed via a peer-to-peer or other lending platform that does not fall within the scope of Regulation (EU) XXXX/ XXX[15] or under any other relevant regulatory framework within or outside the EU and, which is notably a decentralized or distributed application with no legal or natural person with control or influence over it.

Please consider our arguments regarding peer-to-peer platforms and DeFi, made above.

XVII. is investing or exchanging crypto assets, which themselves entail privacy-enhancing features or offer a higher degree of anonymity (such as privacy coins) or the customer receives crypto assets which have been subject to privacy-enhancing activities, in particular processes which obfuscate the transaction on the ledger technology or contain other characteristics similar to those listed in point

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

a) of guideline 21.5.

Please consider our arguments regarding the privacy tools, made above, as well as the contents of the attached document.

XVIII. repeatedly receives crypto assets from or sends crypto assets to:

a. a crypto asset account through an intermediary service provider, which does not fall within the scope of Regulation (EU) XXXX/ XXX[16] or under any other relevant regulatory framework within or outside the EU; or which is subject to AML/CTF regulatory and supervisory framework that is less robust than the one provided for in Directive (EU) 2015/849;
b. multiple self-hosted addresses or multiple addresses located in other CASPs;
c. a newly created crypto asset account or a distributed ledger address held by a third party;
d. self-hosted addresses on decentralised platforms, which involve the use of mixers, tumblers and other privacy enhancing technologies that may obfuscate the financial history associated with the distributed ledger address and the source of funds for the transaction, therefore undermining the CASP's ability to know its customers and implement effective AML/CTF systems and controls;
e. a crypto asset account shortly after being onboarded by the CASP, which is then followed by a withdrawal from the customer's account in a short period of time;

Many of the examples, provided in this Guideline have already been discussed above. However, Guideline 21.5. b) XV e) requires further attention, as what is described is a common low-risk used behaviour case of a transfer after a transaction eg. sell or buy of crypto assets - a crypto asset account shortly after being onboarded by the CASP, which is then followed by a withdrawal from the customer's account in a short period of time. This does not represent a risk as clients often move the assets to their wallets.

Regarding guideline 21.7

We consider that Guideline 21.7 a) includes the undefined phrase "personal or business link", and that it is unclear what "links" mean in this particular context, as the source of funds is checked through EDD. We suggest either clarifying the meaning of the sentence or deleting it as the main purpose of the source of funds check is to verify the origin of assets.

Regarding c) We suggest deleting the expression "links" (with a jurisdiction associated with an increased ML or TF risk) as it is unclear what such links should represent and how such information can even be obtained in practice.

European Crypto Initiative

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

Regarding guideline 21.12,

As a general comment, we'd like once again to raise the issue of the importance of the right timing when updating these Risk Guidelines - and particularly their alignment with tall the files from the AML Package.

> C. obtaining more information about the customer and the nature and purpose of the business relationship to build a more complete customer profile, for example by carrying out open source or adverse media searches or commissioning a third-party intelligence report. Examples of the type of information CASPs may seek include:

IV. information on any associations the customer might have with other jurisdictions (headquarters, operating facilities, branches, etc.) and the individuals who may influence its operations;
We suggest excluding the "individuals who may influence its operations" from the Guideline, as it is unclear what is meant by this. The management board members are identified as well as UBOs, thus we consider it too broad and unspecified to encompass all potential "individuals who may influence its operations" without these individuals posing any significant level of risk. It is also unclear what operations represent in this context (financial, day-to-day, with strategic implications, etc.).

> V. to request or obtain data relating to the customer's crypto asset transaction and trading history.

Regarding this Guideline, we suggest expanding what is meant by "trading history" by explaining whether what is meant is providing evidence considering the source of crypto assets, or if the scope is more general. If the latter is the case, then we consider that such a measure will not be adopted in practice due to its high intrusiveness. Furthermore, if "to request or obtain data relating to the customer's trading history" is applied to trading outside the CASP system, we suggest its deletion due to the same reasoning.

The European Crypto Initiative is a Brussels-based trade organisation that supports innovative & innovation-friendly regulation adapted to decentralised applications that leverage blockchain technologies. We believe it would be beneficial to continue this conversation, provide you with further details and comments and hear your opinion and concerns. Please feel free to contact us so we can set a meeting at your convenience: info@crypto-initiative.eu.