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

Consultation Response by the Digital Currencies Governance Group

About DCGG

Digital Currencies Governance Group (DCGG) is a trade association that represents digital assets issuers and service providers in the European Union and the United Kingdom. Our mission is to facilitate an open dialogue and encourage communication between policymakers and digital asset experts to support the design of a sound and proportionate regulatory framework that ensures safety for all market participants.

Our Members include Tether - currently the largest stablecoin issuer worldwide, Ledger - a leading technology service provider for self-custody, Bitfinex - a major centralised crypto-assets exchange, ZKValidator (ZKV) - a leading proof-of-stake validator, and Iden3 - a solutions provider for self-sovereign identity management. Our team of former government officials, lawyers, and cryptoasset experts regularly engage with policy-makers and regulators both at the national and international level. For any general enquiries or to request further information, please do reach out to info@dcgg.eu.

Consultation questions

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

DCGG and its members have no comments and agree with the proposed changes to this section of the amended guidelines.

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

Regarding the amendments to Guideline 1, DCGG and its members agree it is sensible that the implementation of a new product, business service or process, and innovative technologies to facilitate the firms' existing AML/CFT system, should be subject to risk assessment using existing global best practices such as those published by the FFIEC. This is already an established practice within the internal controls and procedures frameworks of compliant CASP, and we believe it would enhance the transparency, effectiveness and longevity of the AML/CFT framework while also welcoming the application of emerging technological solutions by CASPs within their ecosystems, products and services.

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

DCGG agrees that the expansion of the scope of Guideline 2.4 in relation to identifying ML/TF risk factors might successfully cover unregulated CASPs that may be exposed to higher risk levels. While the alignment with the amended Guideline 9.21 is sensible, we are concerned that this alignment, as it currently stands textually, would entail a due diligence process that

might be too onerous for CASPs to comply with in terms of identifying risk factors for all third-country and/or unregulated customers they interact with. We recommend further specifications to this amendment to state that this risk factor should be subject to a risk-based approach rather than being set as a regulatory requirement for all such interactions. This is in accord with the technological capabilities that blockchains offer which allows for counterparty risk assessments based on blockchain tracing and risk rating software which publish whether a service is known to interact with known high-risk wallets. Such risk assessment techniques are not available for traditional financial institutions but are part of the value proposition of cryptocurrencies.

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

In relation the amendments to Guideline 4 (*CDD measures to be applied by all firm*s) - DCGG and its members would like to offer the following comments:

- **Unusual transactions**: According to the amendments to Guideline 4.60 a), firms would be subject to expanded requirements for detecting unusual transactions or pattern of transactions to initiate an enhanced due diligence (EDD) process. We believe this is sensible given the evolving nature of the crypto-asset ecosystem and the use-cases of crypto-assets and the manners in which users transact with them. Nevertheless, we believe more detailed guidance would be helpful in relation to "successive transactions without obvious economic rationale" and if the EBA would be developing a separate set of guidance or methodology for obliged CASPs to objectively assess the economic rationale (or lack thereof) of successive transactions in order to comply, increase the effectiveness of unusual transaction monitoring and adequately apply EDD measures. This is because we believe that "successive transactions without obvious economic rationale" does not by itself denote high risk activity in absence of other red flags.

- **Transaction monitoring:** The amended Guideline 4.74 d) outlines that firms must determine whether the use of advanced analytics tools (e.g., Blockchain analytics) is necessary in their transaction monitoring processes in light of ML/TF risk associated with the business and customers' transactions. We fully support the use of DLT to facilitate, where relevant, real-time or ex-post transaction monitoring. If applied on a risk-sensitive basis and taking into account the nature, size and complexity of the business, we believe the employment of Blockchain analytics would significantly improve firms' transaction monitoring procedures through transparency, immutability and traceability. CASPs would be able to use these analytics tools to risk-assess incoming and out-going funds, as well as freeze funds in cases of suspicious transfers, conduct internal investigations and file suspicious activity reports.

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

DCGG strongly supports the amendments proposed in relation to Guideline 6 on the requirements for adequate training of obliged entities' staff. A majority of crypto market participants, including our members, ensure that their staff possesses sufficient technical knowledge to facilitate the firms' operations and services and is well-prepared to react in the

event of ML/TF risk being identified and/or mitigated. We support the requirement for sound technical understanding of the firms' product and services by designated staff, as well as the use of advanced analytics tools for transaction and business relationship monitoring to protect users.

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

In relation to the amendments to Guideline 8 (*Sectoral guideline for correspondent relationships*), DCGG would like to offer the following comments:

- **Customer risk factors**: According to the amended Guideline 8.6 d), engaging in corresponding relationships with third-country providers that are not regulated under MiCA or any other relevant EU regulatory framework, or are subject to an AML/CFT regime that is less robust than AMLD VI, could be treated as higher risk. The guidance does not currently specify which EU regulatory frameworks would be considered equivalent to MiCA for the purposes of this section of the guidance, nor how obliged entities should determine the robustness of the AML regime to which respondents are subject to. As a result, there is a need for specific guidance on the scope of the proposed amendments to Guideline 8.6.

  In our view, the EBA should take into consideration that the MiCA regulation at this stage only governs certain market participants (e.g., stablecoin issuers, CASPs), while other assets or providers that are either emerging, or fulfil a different consumer demand/use-case are not subject to these requirements. Treating such entities as higher risk in principle would therefore be premature - it would create undue burden for CASPs engaging in correspondent relationship in terms of due diligence, and it might also prompt a more discriminative approach to non-MiCA regulated service providers and dis-incentivise them from engaging with EU-regulated entities. Given the cross-border nature of the sector, such a result could lead to loss of capital and stifling the development of the European crypto-asset market.

  With regard to the AML/CFT regime that third-country respondents are subject to, we would like to highlight that, at present, there is not full harmonisation of AML rulebooks at an international scale. The work of international standard-setters such as the Financial Action Task Force (FATF) is becoming increasingly adopted and transposed into statutory legislation, however the level of transposition might vary from jurisdiction to jurisdiction depending on national policy priorities. We recognise that it is important that the AML regime governing a third-country provider is effective enough to ensure the risk in correspondent relationships is reduced, and we view as necessary that further guidance is put forward in relation to assessing the 'robustness' of an AML regime in order to address potential divergences and nuances, and promote legal clarity for obliged entities. We also note, though, that third-country respondents are not only scrutinised through their local laws and regulations, but also by the large global banks which facilitate correspondent banking services. Such banks often impose global best practices on their customers which effectively raises the standards of the compliance programs globally.

Furthermore, the amended guideline states that risk factor assessment requirements would also be applied to respondents conducting business on behalf of CASPs which allow transfers to and from self-hosted wallets. While we understand that self-hosted wallets and their anonymity aspect has been seen as concerning by policymakers, we believe it is necessary that the proposed guidance makes the necessary contrast between different types of wallets. For example, software self-hosted wallets and hardware self-custody wallets carry very different risk levels based on their features and functionalities. The former is software-based which makes it more prone to hacks (as these provide access to users' assets), theft or similar illicit activity, while the latter (which allows for storing assets completely offline) provides greater consumer safety and is therefore a lesser requirement for regulation and/or perceived higher risk level under these ML/TF Guidelines. Based on this, depending on the type of wallet involved in the respondent's interaction with the obliged entity, risk levels could vary significantly.

Therefore, we recommend that risk factor assessment in the context of correspondent relationships with providers that enable self-hosted wallet transfers is subject to a risk-based approach, taking into account the type of wallet involved. This would also mean that if the origin of the wallet cannot be verified with a sufficient level of certainty, and there is suspicious activity involved, the interactions would be considered high risk. If that is not the case, we believe it is sensible that self-hosted wallets are not subject to a discriminatory approach, given the important part they play in the crypto ecosystem.

Overall, while the factors outlined by the EBA might contribute to increased risk levels in correspondent relationships, we recommend that the EBA takes a more nuanced approach in order to allow the market to develop. With this in mind, we welcome a revision of the proposed amendment, or further clarifications on the matters outlined above.

- Respondents based in non-EEA countries: With respect to the amended Guideline 8.17 for compliance with Article 19 of Directive (EU) 2015/849, when entering into a cross-border correspondent relationship with a non-EEA/third-country respondent institution, obliged entities would have to make additional assessments to ensure risks are mitigated in such scenarios. Guideline 8.17 c) states that obliged entities should conduct a qualitative assessment of the AML/CFT framework of the third-country respondent beyond their AML policies, including assessing the transaction monitoring tools in place to ensure that they are adequate for the type of business carried out by the respondent. In practice, we view that this requirement would be extremely onerous for obliged entities, mainly because a non-EEA CASP is not required by law to disclose their AML controls and transaction monitoring tools where no business agreement exists between them and the EU CASP. If this requirement remains as it currently is, EU-licensed CASPs might have to stop transfers if the respondent party does not disclose this information, which could lead to significant disruption of the EU marketplace, given the cross-border nature of the sector. Based on the above, we

recommend that the caveat is added to the amended section of the guideline to ensure clarity and proportionality and to reduce the administrative burden on obliged entities:

"c) Assess the respondent institution's AML/CFT controls. This implies that the correspondent should carry out a qualitative assessment of the respondent's AML/CFT control framework, not just obtain a copy of the respondent's AML policies and procedures. This assessment ***could*** *include****, provided that the information can be obtained,*** *the transaction monitoring tools in place to ensure that they are adequate for the type of business carried out by the respondent."*

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

In relation to the amendments to Guideline 9 (*Sectoral guideline for retail banks*), DCGG would like to offer the following comments:

- **Pooled accounts**: We support the application of simplified due diligence (SDD) by retail banks with regard to compliant firms or customers that carry low risk levels, based on the assessment methodology outlined in EBA/GL/2021/02, rather than the nature of their activities or services offered. As long as firms adequately comply with the relevant guidelines for pooled/omnibus accounts, we foresee that a SDD approach would be proportionate.

- **Customers that offer services related to crypto-assets**: We would like to highlight that, while banks' correspondent relationships with third-country CASPs not regulated under MiCA carry specific considerations given the differences in governing international regulatory frameworks (i.e., such CASPs have not undergone the disclosure procedures set out in MiCA), we would like to encourage banks not to prematurely adopt a more discriminative approach to such CASPs in terms of perceived risk levels. As mentioned in our response to Question 6, MiCA authorisation only applies to specific providers under its remit, and the lack of such authorisation can be attributed to a variety of factors such as costs, transitional periods, or products and use-cases not falling under MiCA scope. We therefore recommend that this assessment is made on a risk-sensitive basis instead of being set as a firm requirement, in order to acknowledge the gaps that currently exist in the regulatory landscape until these are addressed in forthcoming legal frameworks.

  Furthermore, under Guidance 9.20, further clarity is needed with regard to which other EU regulatory frameworks would be considered as relevant and/or equivalent to MiCA in the context of the risk level assessment requirement, as this is necessary for promoting legal certainty. We would also welcome guidance regarding what the intention is behind the caveat *"banks should also consider the ML/TF risk associated with the specific type of crypto assets",* and what the EBA would consider the current risks are in relation to different types of crypto-assets, in order to avoid a potentially uninformed or discriminatory approach to certain assets in the ecosystem.

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

DCGG and its members have no comments and agree with the proposed changes to this section of the amended guidelines.

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

The new Guideline 21 (*Sectoral guidance for crypto asset services providers*) sets out considerations on crypto sector-specific risk factors and their assessment. While we recognise that the underlying technology of crypto products and services carries its benefits and risks and a significant part of the requirements under this Guideline reflect this adequately, we believe that certain provisions under this section could result in harm to the industry's development and positioning in the EU market, as well as excessive administrative burden for CASPs in conducting risk assessment. Based on this, DCGG and its members would like to highlight the following issues that merit further consideration or clarification by the EBA:

- **Product, services and transaction risk factors**: According to the provisions set out in Guideline 21.3, products that allow interactions with self-hosted addresses, non-MiCA/EU framework-regulated service providers, third-country service providers and decentralised finance (DeFi) applications may be considered as factors contributing to increased ML/TF risk. As mentioned across our responses to the previous questions in this consultation paper, we disagree with the notion that such transactions are inherently higher risk than others, as there are diverging reasons as to why these activities or interactions are currently outside of the regulatory scope of a bespoke framework. Particularly in the case of DeFi, the lack of regulatory framework on a European or international level is primarily due to the fact that regulators have not yet endeavoured in putting forward a comprehensive DeFi legislative framework. This does not necessarily mean that DeFi applications are riskier than CeFi, as we recognise that this strand of the sectors carries its own benefits and risks. Nevertheless, our view is that the interactions above should only be deemed high risk when monitored on a risk-sensitive basis and suspicious activity is flagged.

- **Risk factors related to the nature of the customer**: Guideline 21.5 sets out that undertakings which are in an intra-group relationship with other crypto-asset businesses would be considered higher risk customers. Further guidance would be welcomed as to what the EBA considers an intra-group relationship in the context of the crypto-asset sector and which relationships with crypto-asset businesses are considered problematic. From our perspective, as long as sound disclosure requirements are in place, this scenario would not inherently be riskier than others.

  The Guideline also lists "a vulnerable person or a person who displays very little knowledge and understanding of crypto assets or the related technology, which may increase the risk that the customer is being used as a money mule" as a factor contributing to increased risk. We recognise and support the EBA's efforts to protect citizens that could be involved in such a situation, however we believe this factor as it currently stands does not provide sufficient legal clarity for obliged entities, and we

welcome further specifications as to how CASPs would be required to assess the vulnerability or lack of knowledge of a person to comply with that provision, especially if the onboarding process already includes an appropriateness/knowledge test.

- Risk factors related to the behaviour of the customer: We agree with the majority of outlined ML/TF risk factors attributed to customer behaviour. Yet, we would like to highlight a crucial point that considering the investment or exchange of crypto-assets borrowed through a decentralised or distributed application with no legal or natural person with control or influence over it a high-risk factor could have a negative impact on the DeFi sector in the EU. Until there is a bespoke framework in place to address DeFi, our view is that it would be premature to deem customer engagement with DeFi-related activities such as the one above as high risk. Furthermore, the absence of a framework for decentralised activities could also make it challenging for CASPs to follow an EDD process that is geared toward centralised issuers and service providers, and meaningfully comply with this Guidance. We therefore recommend that this piece of the guidance is revisited and potentially removed until DeFi impact assessment reports and any forthcoming legislative frameworks have been comprehensively developed.

  Of note: According to the recently published recast of the Transfer of Funds Regulation (Regulation (EU) 2023/1113), a de minimis threshold (e.g., 1000 EUR) as part of the Travel Rule has not been defined and is not a part of the forthcoming EU cryptoasset transfer provisions. Therefore, the requirements set out in Guidelines 21.5.b)vii.) and 21.5.b)xv.)f) that make references to the threshold set out in the TFR, should be amended to reflect the provisions in the Regulation, or deleted entirely to avoid regulatory ambiguity for obliged entities.

- Country or geographical risk factors: With regard to Guideline 21.7 on geographical risk factors which states that if the originating or the beneficiary crypto asset account or a distributed ledger address is linked to a jurisdiction associated with a weak AML/CFT regime, it could be considered as higher risk. To reiterate our position as posed in question 6, we would welcome any guidance on a potential set of minimum objective criteria that should be employed by obliged entities to determine the weakness or robustness of an AML/CFT framework for the purposes of facilitating compliance with country-related provisions and promoting clarity.

- Distribution channel risk factors: Guideline 21.9 outlines that new distribution channels or new technology used to distribute crypto-assets that have not been fully tested yet or used before may contribute to increasing risk. DCGG would like to note that we support this provision with regard to distribution channels that have not undergone the necessary tests prior to their launch, however we disagree that new technologies (i.e., that "have not been used before") carry an equal level of risk. In our view, new distribution channels or technological tools for distribution do not necessarily carry higher risk, especially when they have undergone the necessary auditing and testing process. We therefore recommend that this latter part ("or used before") is removed

from this section of the guidance for the purposes of proportionality and technological neutrality.

- **Enhanced customer due diligence**: DCGG views the majority of the proposed EDD measures under Guideline 21.12 as sensible and in line with the realities of the sector and potential ML/TF risk concerns. Yet, to ensure that disproportionate and undue administrative burden is not placed on CASPs to an extent that either their daily operations are disrupted, or that excessive costs are involved, we would like to shed light on certain issues in the EDD provisions that could lead to these undesired outcomes.

  We have identified that the requirement for carrying out open source or adverse media searches, as well as commissioning a third-party intelligence report to comply with the provisions laid out in Guideline 21.12 could be extremely onerous, especially when dealing with a high volume of transactions, either as a part of a business relationship or occasional transactions. Specifically, investigating the source of wealth, purpose of the transaction or information on associations with other jurisdictions will not necessarily be public information, and commissioning an intelligence report could be a costly process, especially if this has to be applied frequently. To mitigate the risk of placing an excessive burden or cost on compliant obliged entities, we believe this section of the guidance should specify that CASPs should apply the relevant EDD measures and obtain more information only to the extent that this is operationally possible. Additionally, from DCGG's perspective, a comprehensive cost-benefit analysis by the EBA on the application of these measures would certainly provide the necessary clarity in relation to the feasibility of the proposed requirements.