DIGITAL CURRENCIES
Governance Group

Guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under Regulation (EU) 2023/1113 ('The Travel Rule Guidelines')

Consultation Paper 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 security technology 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.

Questions for consultation

Question 1: Do you agree with the proposed provisions? If you do not agree, please explain how you think these provisions should be amended, and set out why they should be amended. Please provide evidence of the impact these provisions would have if they were maintained as drafted'?

The Digital Currencies Governance Group (DCGG) welcomes the opportunity to provide feedback on the European Banking Authority's (EBA) proposed Guidelines (GL) on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing (ML/TF) purposes under the recast Transfer of Funds Regulation (Regulation (EU) 2023/1113). As crypto-asset service providers (CASPs) and intermediary crypto-asset service providers (ICASPs) are now being brought within the remit of the transaction traceability requirements under the previous iteration of the Transfer of Funds Regulation (Regulation (EU) 2015/847), it is crucial that an appropriate balance is struck between strengthening the EU's AML/CFT framework, protecting European consumers, and fostering innovation within the ever-evolving EU crypto sector. This can be achieved by facilitating a smooth transition for CASPs to comply with the principles outlined in the draft GL, ensuring that excessive or disproportionate burden is not placed on reporting entities.

To this end, as a trade association representing digital asset issuers and service providers, we are pleased to outline our perspectives on the EBA's proposed Travel Rule Guidelines, with the objective to promote a level-playing field between entities in scope of the Transfer of Funds Regulation (TFR).

General feedback

Overall, we recognise the EBA's efforts to clarify the steps CASPs and ICASPs should take to detect missing or incomplete information in a crypto-asset transfer, and procedures in place to manage crypto-asset transfers lacking the information required by the TFR Level 1 text. Although we strongly oppose the misconception that cryptocurrencies are primarily used for criminal purposes[1], we believe that the EU crypto-asset industry can play a pivotal role in ensuring that it is not utilised for ML/TF considerations, as long as it does not suffer from a biased, discriminative approach compared to the traditional financial system. While we view a large part of the proposals as sensible and line with the FATF and what requirements other jurisdictions enforce in relation to missing or incomplete information, we believe some provisions could be clarified further or amended in a manner that is proportionate to the newly regulated status of CASPs and ICASPs, as well as the technological and operational realities of the sector, notably when it comes to the use of self-hosted solutions. DCGG would like to highlight the importance of refraining from gold-plating in adapting the FATF guidance so as to avoid regulatory and supervisory discrepancies with other jurisdictions. We outline our views on specific sections of the draft GL in more detail in our response below.

Guideline 3: Transmitting information with the transfer (Article 4, Article 5, Article 6 and Article 14 of Regulation (EU) 2023/1113)

In relation to Guideline 3.1 on the use of messaging systems, we welcome the proposed transitional period for CASPs and ICASPs, whereby entities are allowed, until July 31, 2025, to use infrastructure or services that are not fully capable of transmitting the required information and require additional or alternative technical solutions to comply with the TFR. We are pleased with the acknowledgement that CASPs and ICASPs, as newly regulated entities under this framework as opposed to PSPs and IPSPs, could face technical limitations in the transmission and reception of information required under this rulebook, and the grace period proposed in these draft Guidelines allows for much needed proportionality for the industry.

In our view, the text does not make it clear whether the the same proportionality for CASPs is extended to the requirements under Guideline 3.3 (*Batch Transfers*) whereby CASPs are required to submit missing information from a batch transfer routed through one or more intermediaries via alternative channel mechanisms (e.g., APIs, third-party solutions). In particular, we are interested to know if, in such scenarios, CASPs are explicitly allowed by these guidelines to test different methods to find out the most effective approach to comply with this requirement in a manner that is consistent with AML/CFT objectives, but also does not put an excessive operational onus on the provider. The industry would benefit from further clarification on whether such flexibility is allowed, and whether any time constraints are present (e.g., not being able to use alternative methods after a grace period concluding on July 31, 2025). In DCGG's view, mandating that CASPs can use different alternative methods that still aid in achieving the desired regulatory objective in relation to batch transfers should be allowed, at a minimum until July 31, 2025.

[1] The latest Chainanalysis report from January 2024 shows that criminal activity constituted just 0.34% of all cryptocurrency transaction volume in 2023, an infinitesimal portion compared to the use of traditional finance and fiat transactions for ML/TF purposes.

Guideline 4: Information to be transmitted with the transfer (Article 4 and Article 14 of Regulation (EU) 2023/1113

We agree with the principle, as part of monitoring obligations, of originator CASPs to issue a warning to the next CASP in the transfer chain in the scenario where missing or incomplete information is detected or an error has been identified post-transaction to ensure the appropriate measures to be taken are clear to the next CASP in the transfer chain. However, we would like to stress that the draft Guidelines should explicitly stipulate that originator CASP should not be held liable in the occasion where the next CASPs in the transfer chain does not fulfil the relevant requirement to obtain the missing information, if it was already informed by the originator's CASP that an error has occurred. Once the information regarding the error has been relayed, the TFR or these Guidelines should not require any further action by the initial CASP in relation to obtaining missing information, as any further action beyond informing the next CASP would be operationally burdensome.

Guideline 5: Detecting missing information (Article 7, Article 11, Article 16 and Article 20 of Regulation (EU) 2023/1113)

As an initial comment, we welcome the flexibility enabled by the proposal under Guideline 5.3. (*Monitoring of transfers*) for CASPs and ICASPs to determine the threshold alerting to the presence of higher risk factors based on the average value of transfers they routinely process and what constitutes an "unusually large transfer" based on the specific business model. Some CASPs within the market do process larger volumes than others, and we believe a proportionate approach would be more effective, rather than setting a common threshold for all CASPs, irrespective of their size.

However, we view some of the proposed monitoring requirements under Guideline 5.3. as unduly discriminatory and thus potentially onerous for reporting CASPs and ICASPs to conduct. We understand that CASPs and ICASPs are required to determine specific risk-increasing factors to facilitate more effective monitoring of transfers and should, for these purposes, also consider **transfers with entities with self-hosted wallets** or **entities based in a third-country that has not implemented a licensing regime** or **does not regulate CASP activity** (paragraph 34(e)).

With regard to self-hosted wallets, we disagree that transfers involving such wallets are, solely by virtue of being self-hosted, higher risk in comparison to transfers involving centralised wallets. If this principle remains in the Guidelines as it is, reporting CASPs and ICASPs would undergo additional administrative burden if they have to conduct enhanced monitoring on all transfers involving a self-hosted wallet, which we see as disproportionate. Instead, we recommend that reporting entities should be required to focus on whether the transaction is suspicious based on more objective factors (e.g., if the transfer is unusually large) in order to effectively safeguard consumers from ML/TF risk. They should not be required to excessively monitor each self-hosted wallet transfer just because it involves a self-hosted wallet, as this may affect their operational capacity, especially for CASPs experiencing large daily volumes.

On a similar note, with regard to transfers involving entities based in a third-country that does not enforce a licensing regime or does not regulate CASP activity, we disagree that this should be a determining factor for enhanced monitoring. Firstly, because the cryptoasset sector is inherently

cross-border, and the possibility of facilitating transfers between jurisdictions that have similar regulations to the TFR in place all the time, is low, and that would therefore entail excessive monitoring of each transfer involving an entity from a third country with a less mature AML/CFT regime, which we believe is counterproductive, and third country entities may generally not necessarily imply higher risk. Indeed, such transfers could lead to vulnerabilities should illicit actors exploit the differences in the strength of the AML framework between the counterparty jurisdictions; yet, our view is that the monitoring requirements should be predominantly based on more objective, quantitative factors (e.g., unusually large transfers, suspicious batches, etc.), similar to our perspective on transfers involving self-hosted wallets. Geography and maturity of the domestic AML regime should be taken into account, but it should not be the main or determining criterion. This way the proposal would avoid taking a discriminative approach toward jurisdictions with less mature AML frameworks (which can be due to a variety of reasons), and more effective monitoring could be conducted by TFR-regulated CASPs and ICASPs with a proportionate administrative burden.

Overall, in DCGG's view, monitoring requirements of transfers with entities with self-hosted wallets or entities based in a third-country that has not implemented a licensing regime or does not regulate CASP activity should be proportionate and more fairness should be given to these entities, as we disagree with the principle that such transfers should automatically be assumed as higher risk by virtue of involving a self-hosted wallet or a third-country entity with a less mature AML regime, and more objective factors should be taken into account instead. Paragraph 36 of the draft Guidelines states:

"*PSPs, IPSPs, CASPs and ICASPs should note that missing or inadmissible information may not, by itself, give rise to suspicion of ML/TF. When considering whether or not a transfer raises suspicion, the PSPs, IPSPs, CASPs or ICASPs should take a holistic view of all ML/TF risk factors associated with the transfer.*"

We urge the EBA to consider giving the same flexibility of assumption to transfers involving the entities outlined above to more effectively mitigate ML/TF risk.

Guideline 6: Transfers with missing or incomplete information (Article 8, Article 12, Article 17 and Article 21 of Regulation (EU) 2023/1113)

DCGG believes that the draft Guidelines related to missing or incomplete information accompanying the transfer is overall sensible, provided that it does not place an undue burden on beneficiary CASPs or ICASPs. Specifically, the GL should ensure that CASPs/ICASPs are not required to undertake disproportionate efforts to verify the completeness and accuracy of the information received beyond requiring the information to be sent from the prior CASP (within the timeframes stipulated in the GL - 3 working days for transfers taking place in the EU, and 5 working days for transfers received outside of the EU) if an error is identified. In addition, we disagree that the same 5-day deadline should be set when there are more than two parties in the transfer flow (e.g., intermediaries, non-banks), as there could be operational challenges in contacting all the parties involved to collect the information, and we believe a deadline of 7 working days might be more effective in such scenarios.

While we agree that the beneficiary CASP or ICASPs should consider the future treatment of PSPs, CASPs, ICASPs or self-hosted wallets, in scenarios where either of these fail to provide the missing information, any requirement to potentially return the funds of the crypto asset or stable coin transaction on the basis of missing transfer information is very problematic and overly burdensome (paragraph 53), as it could easily to lead to fraud from payers, who could attempt to buy products, providing incomplete information for a crypto asset or stablecoin transaction.

Furthermore, the requirements for requesting missing information should not be operationally onerous or costly, especially for larger CASPs that process a high volume of transactions. We echo this view specifically on paragraph 55 in Guideline 6.6. *(Contacting the prior PSP, IPSP, CASP and ICASP in the transfer chain)* whereby CASPs would be required to send requests for missing information from transfers involving self-hosted wallets directly to the customer. Irrespective of the result, we believe the more proportionate approach would be that no liability is placed on TFR-regulated entities beyond issuing the request.

As a general clarification, CASPs could benefit from the inclusion of information pertaining to the specific steps that CBs are expected to take when the information received from the originator does not match their records within the Guidance. This would help to ensure that CASPs are able to comply with the GL in a consistent and efficient manner.

Guideline 8: Transfers of crypto-assets made from or to self-hosted addresses (Article 14 (5) and Article 16 (2) of Regulation (EU) 2023/1113)

DCGG disagrees with the notion of self-hosted wallets posing “potential high risks” or representing a greater “technological and regulatory complexity” in mitigating ML/TF risks compared to other digital asset solutions on the market, which is not based on any actual empirical data. They should not, by nature, be discriminated against when it comes to ML/TF considerations.

In addition, in DCGG’s view, some of the proposals regarding transfers of crypto-assets made from or to a self-hosted addresses under Guideline 8 could give rise to an excessive administrative burden for CASPs, specifically in terms of assessing risk when detecting missing information, identification requirements and obtaining proof of ownership or controllership of a self-hosted address.

Firstly, we believe the rationale outlined in Guideline 5.1 (*Procedures to detect missing information*), whereby CASPs should determine the criteria that alerts to risk-increasing factors based on the nature of their business and daily volume, should also be applied to the processing of transfers involving self-hosted wallets. Such transfers should not be considered higher risk by nature and, when in cases of missing or incomplete information, should not be treated automatically as such to avoid a discriminatory and unduly complicated approach. Instead, they should be assessed against objective quantitative criteria (e.g., unusually large value of the transfer, linked transfers, frequency, etc.), such as the one set out by CASPs for risk-increasing factors. This would avoid discriminating against self-hosted solutions and placing a disproportionate burden on CASPs to approach all incoming self-hosted wallet transfers as higher risk, which can be especially challenging to handle from a technical perspective for CASPs that process large daily volumes. Instead, we support a pragmatic, risk-based approach, similar to the rationale stipulated by Guideline 8.2.4 (*Mitigating*

measures to put in place regarding transfers from or to a self-hosted address): "*CASPs should apply enhanced due diligence measures to transfers involving self-hosted addresses which present a high risk of ML/TF*".

Secondly, we understand that Guidelines 8.2.1. and 8.2.2. require CASPs to rely on available technical means to collect information and identify a transfer involving a self-hosted wallet, as well as identify the originator and beneficiary in such transfers. We would like to highlight that some requirements, such as using third-party data providers to identify the self-hosted wallet holder (which could be costly) or going directly to the customer if technical means for identification are insufficient (which is operationally onerous when processing high daily volumes), are disproportionate in comparison to what is applied and required in cases of transfers centralised wallet addresses only, and unnecessary. These identification requirements could be seen as helpful in the objective of more transfers in the EU becoming transparent, but they would broadly diverge from common supervisory practices in the field across the globe.

Furthermore, it is important to acknowledge the economic and operational realities of the sector, as CASPs are capable of checking if the transaction information has been received. The receiving centralised wallets may not be completely capable of identifying or verifying the accuracy of transactions from unhosted wallets without both the CASP and the consumer being severely encumbered by this requirement. If the requirements are not applied proportionately, this may risk circumventing broader regulatory standards by using non-EU compliant/regulated CASPs for transfers. In turn, this would pose additional enforcement difficulties for the EU, given the limited cross-border enforcement capacity, and would put EU CASPs at a competitive disadvantage vis-à-vis their international competitors. Therefore, we believe the CASP receiving the information should only be obligated to assess its completeness.

Finally, in line with the reasoning outlined above, we view the requirements for verification of ownership under Guideline 8.2.3 (*Transfers above 1 000 EUR and proof of ownership or controllership of a self-hosted address*) as extremely difficult to apply in practice and do not adequately reflect the realities of how CASPs work, especially larger entities that process multiple daily transactions that may go beyond the suggested 1 000 EUR threshold. The majority of the methods for verification of ownership outlined would require disproportionate efforts to be made by CASPs and this burden would be further exacerbated if a combination of more than two methods, as stipulated in paragraph 6, is required, and would be operationally very challenging to achieve. In our view, CASPs should be allowed flexibility to choose a method of verification of ownership/controllership of a self-hosted address beyond what is set out in this Guideline if impossible to achieve from an operational standpoint. The industry is constantly developing innovative methods that could be more effective in achieving this objective without putting an excessive operational onus on CASPs, and we believe this Guideline should be more technologically neutral to allow for the use of verification methods to be developed by the industry that both fulfil the AML/CFT objectives set out by this regulation and do not excessively encumber regulated CASPs.

Impact assessment

DCGG acknowledges the efforts put forward by the EBA to formulate these draft Guidelines under the TFR mandate, and the reasoning outlined in the Impact Assessment section of the GL, and the Options considered. However, while we understand the rationale and objective of "greater regulatory certainty" regarding Option 1.1 ("*The EBA could focus on the articles listed in the mandate and to other articles where this is necessary to ensure the consistent application of the Regulation's obligations")*, we are concerned that this Option, currently retained under the draft FL, seems to advantage PSPs/IPSPs already regulated by the EU ML/TF framework in terms of one-off costs incurred over CASPs/ICASPs which would have to implement the proposed systems and controls from scratch to comply with this Regulation. Importantly, these entities are just starting to become regulated under new EU files - the TFR and the Markets in Crypto-Assets (MiCA) Regulation. The text states that the costs for PSPs/IPSPs are expected to be absorbed by the modifications of the underlying ML/TF framework, but does not reference the implications for CASPs/ICASPs. We are therefore particularly concerned that the proposal, as it currently stands, appears to favour incumbent market participants in managing their compliance obligations, and fails to acknowledge the higher costs incurred (or clarify the expected costs) for newly regulated entities. This demonstrates a lack of a level-playing field between the entities in scope, yet we believe this is crucial for proportionality and the principle of non-discrimination.

Option 1.2 ("*The EBA could write guidelines exclusively on the articles listed in their mandate")* seems to better reflect the implications of increased compliance costs for CASPs/ICASPs and is limited to the mandate given by the TFR. We believe the EBA should revisit the options considered and aim to provide better clarity within the limits of their mandate, as indicated under Option 1.2, and still achieve consistency and prevent regulatory arbitrage and diverging interpretation. We believe this could be achieved through further engagement with industry stakeholders and experts, without imposing excessive compliance costs to CASPs/ICASPs.

We at DCGG stand ready to discuss this further with you, so as to ensure that we put forward realistic solutions that balance innovation in the EU crypto sector with the need for financial integrity in the fight against ML/TF practices.