ABI Associazione Bancaria Italiana

CONSULTATION PAPER ON THE

DRAFT 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')

ABI's response

8 February 2024

POSITION PAPER

2/2024

The Italian Banking Association (ABI) would like to thank the European Banking Authority (EBA) for providing the opportunity to comment on the draft guidelines through which the EBA aims to promote the development of a common understanding of effective procedures to detect and manage the transfer of funds and crypto-assets lacking the required information, according to Regulation (EU) 2023/1113 ("Regulation").

1. General remarks

ABI supports these draft guidelines setting out in detail what payment service providers (PSPs), intermediary PSPs (IPSPs), crypto-asset service providers (CASPs) and intermediary CASPs (ICASPs) should do to comply with Regulation. Indeed, a common understanding is essential to ensure the consistent application of EU law and to contribute to a stronger European AML/CFT regime.

ABI considers it important to uphold the principle of "same activities, same risk, same regulatory outcome," as applying consistent rules to both funds and crypto-assets can yield different results. Therefore, certain provisions suggested by the EBA that vary based on whether funds or crypto-assets are transferred have been positively acknowledged. However, we underlined the difficulty in applying the information obligations and checks for CASPs. We anticipate that the difficulties may arise in applying the rules to crypto-assets transfers due to some of the specificities inherent to the technology and precisely as a result of the way in which transfers are made.

As known, FATF has started a review of Recommendation no.16 (Wire Transfers) to examine areas in which R.16 may need adjustment to reflect changes in market developments, to avoid loss of relevant information, and to better meet the objective of the recommendation itself. The scope of R.16 as well the content/quality of the information that must accompany the transfer of funds – among other issues – are under discussion and this would have an impact on Regulation (EU) 2023/1113 and on the related EBA's guidelines. In light of the above, we hope that actions envisaged at the international and European levels will be consistent and harmonized as far as possible, avoiding

the need for continuous and expensive impacts on all the stakeholders to whom these draft guidelines are addressed.

From a strictly formal point of view, we point out that the organization of paragraphs/guidelines is not clear to the extent that the numbering of each guideline remains sequential in general terms and therefore disconnected from the numbering of paragraphs/macro topics covered by the draft guidelines. Moreover, it is not easy to distinguish new guidelines with respect to the ones that already exist but are rephrased.

2. Detailed comments

2. Subject matter, scope and definitions

We suggest clarifying that rejected, returned or recalled transfer of funds (R-transactions) don't constitute a new transfer of funds within the meaning of Article 3 of the Regulation and hence that the requirements of the same Regulation should not apply to such R-Transactions. Indeed, R-Transactions are to be considered as exceptions pertaining to the original payment transaction for which such obligations have been already met.

A new paragraph **9A. Exception handling" should be added to clarify that** "The exceptions pertaining to a transfer of funds (Reject, Return or Recall transactions) don't constitute a new transfer of funds in the scope of Regulation (UE) 2023/1113.

This proposal will avoid unnecessary frictions in the handling of R-Transactions.

4. Preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes

- **Exclusion from the scope of Regulation (EU) 2023/1113 and derogations - Guidelines 2.1 – para. 4**

The objectives that this draft guideline intend to pursue are clear and can be agreed upon. However, it cannot be assumed that a card, an electronic money instrument, a mobile phone or any other digital or IT

prepaid or postpaid device with similar characteristics, is used for the purchase of good or not by applying the suggested criteria.

Therefore, we believe that this draft guideline will require significant effort to the PSPs while not allowing them to unambiguously identify whether the transfer of funds is in scope of the Regulation or not (according 2(3) point (a) and (5) point (b)).

- **Information to be transmitted with the transfer (Article 4 and Article 14 of Regulation (EU) 2023/1113) - Guidelines 4.2. – para. 22**

We suggest verifying if the reference to "paragraph 13" in point 22 is correct. In fact, para. 13 refers to the transfer of crypto-assets while para. 22 refers to the transfer of funds.

Furthermore, we do not find the draft guideline under letter b) for legal persons, according to which "*Where technical limitations referred to in paragraph 13 exist which do not allow the transmission of the full registered legal name, the payer's PSP and the originator's CASP should transmit the trade name*" correct. We believe that the trade name can't replace the legal name for the purposes that this Regulation aims to achieve. In case of technical limitation, a truncation of the legal trade name would be a preferable solution also considering that this hypothesis seems very remote to happen; the number of characters that can admit this information in the payment messages is usually quite extensive.

In addition, in relation to all DLT refinements, the draft guidelines should include criteria and georeferencing forecasts of the DLT itself. The reason for the specification is to be able to detect crypto-assets activities in sanctioned countries, affected by AML/FS/CFT operating restrictions or careless.

- **Information to be transmitted with the transfer (Article 4 and Article 14 of Regulation (EU) 2023/1113) - Guidelines 4.3. – para. 26**

In relation to Article 4.1 c) and Article 14.d) of the Regulation, the draft guidelines should specify:

a) whether the data indicated (the address including the name of the country, the official personal document number, the customer identification number, the date and place of birth) are 1) all alternative to each other, i.e. the presence of any of them is sufficient to fulfil the requirement; or 2) some are mandatory (to be clearly stated) while the remaining are alternative; or 3) they are all mandatory;

b) what is meant by "customer identification number".

Failure to specify the expected data could lead to an uneven interpretation of the rule.

We would also draw attention to the fact that draft guideline no. 26 would appear to be at odds with the regulatory requirement: in fact, it indicates that "*the payer's PSP or the originator's CASP should transfer the information on the date and place of birth in addition, to the address and official personal document number"* while article 4.1. c) and 14. e) states that "*the payer's address including the name of the country, official personal document number and customer identification number, or, alternatively, the payer's date and place of birth*".

In relation to Article 4.1 d) and Article 14.e) of the Regulation, the draft guidelines should specify:

a) whether with the indication "subject to the existence of the necessary field in the relevant payments message format […]" the regulation limits the control over the LEI code only to the type of messages that dedicate a specific/structured field to the LEI code (consequently excluding SWIFT MT, where a dedicated LEI field is not present: it is present only for option F a row 6 where it is possible insert a generic Customer Identification Number).

b) if the "BIC" code can be considered as an equivalent official identifier of the LEI code when the payer or payee of a transfer of funds is a PSP.

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

Guidelines suggest the behaviour and actions that a Crypto-Asset Service Provider (CASP) is required to adhere to in the case of a

transfer lacking necessary information under the FTR, specifically in the context of transfers with incomplete or missing information. Despite the awareness that FTR uses the term "reject" multiple times to indicate one of the options available to the PSP/CASP of the beneficiary when receiving funds or crypto-assets for its client, we believe that the term does not accurately reflect a feasible option for transfers involving crypto-assets, in light of the fact that in the absence of intermediaries there is no acceptance or rejection of a transaction.

If the transfer is authorized by the CASP of the originator because, in its assessment, all information is complete, the order is recorded on the blockchain, and once confirmations are received from validators, the crypto-assets are "credited" to the beneficiary's account. In this mechanism, the CASP of the beneficiary cannot intervene to "reject" a transfer of crypto-assets once written in the ledger and, therefore, cannot reject it.

Having said that, we believe it would be appropriate to clarify whether the term "reject" refers to the described dynamics, and if so, we consider it useful to use more suitable terms – also used by FTR and the EBA in the draft guideline 66 – such as "return" or "not making the crypto-asset available to its client".

In connection with the possibility of returning crypto-assets to the CASP of the originator or to a self-hosted wallet, another critical issue should be addressed. In both cases, the question arises as to who would be responsible for paying the fee associated with the return of crypto-assets (e.g., gas fee). If the CASP of the beneficiary has concluded that the received information is incomplete or untrue (in the case of involvement of another CASP) or cannot demonstrate the identity of the involved party (in the case of a transfer from a self-hosted wallet - please refer to the following points for this difficulty), who should bear the costs of the network fee? Is it possible to deduct both the operational costs and the network fees that the CASP should incur for the return from the crypto-assets of the transferor? In case of disputes, what liabilities could be attributed to the CASP for not completing the transfer or for reversing the crypto-assets?

- **Detecting missing or incomplete information after executing a transfer (Article 8(1), Article 12, Article 17(1), and Article 21 of Regulation (EU) 2023/1113)**

According to article 14, paragraph 5 of FTR, in the case of a transfer of crypto-assets made to a self-hosted address, the crypto-asset service

provider of the originator shall obtain and hold the information referred to in paragraphs 1 and 2 and shall ensure that the transfer of crypto-assets can be individually identified. Also, article 14, paragraph 6 of FTR states that "Before transferring crypto-assets, the CASP of the originator shall verify the accuracy of the information referred to in paragraph 1 on the basis of documents, data or information obtained from a reliable and independent source".

Having said that, draft guideline 55 suggests that in case of missing info or clarification with respect to trasfer from or to self-hosted addresses, the request should be sent directly to the CASP customer. It should be noted that the requests for missing information or clarification about a transfer involving a self-hosted address should affect only the transfer made from a self-hosted address and not also the transfer made to a self-hosted address. In the former case, the request should be sent directly to the customer (draft guidelines 66 of EBA/CP/2023/35) whereas in the latter case, there should be no request of integration, as in such cases, the CASP should neither initiate nor execute the transfer after a missing and/or incomplete information assessment.

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

Draft guideline 67 addresses transfers in crypto-assets with a value below 1,000 EUR occurring between addresses hosted by Crypto-Asset Service Providers (CASP) and self-hosted addresses. Specifically, the provision advises originator and beneficiary CASPs to use suitable technical means to cross-match data, including blockchain analytics and third-party data providers, for the purpose of identifying or verifying the identity of the originator or the beneficiary. In our understanding, it is unclear whether blockchain analysis tools, such as *Chainalysis*, which are mainly designed to evaluate the risk associated with addresses engaged in blockchain transactions linked to illicit or high-risk activities (such as mixers, sanctioned addresses, illicit merchants, etc.), can identify and verifying the identity of originator and beneficiary. It would only be possible, in some cases, to identify through such blockchain analytics whether certain addresses are controlled by a CASP (guide laid down in draft guidelines 65 and 66). Additionally, there is no indication that databases (or services) of "on-chain" addresses, whether public or provided by private third parties, are available for secure and effective consultation to ascertain the identity of the address owners. Hence, we kindly request the Authority

to explain in the final guidelines how the mentioned solutions are suitable for unambiguously identifying address owners. Additionally, the EBA should specify which databases, whether publicly available or provided by third parties, are being alluded to in this context.

Guideline 69 addresses transfers of crypto-assets above 1,000 EUR occurring between addresses hosted by CASP and self-hosted addresses. In particular, the provision calls for the CASP of the beneficiary or the originator to use at least two technical solutions, among those indicated in the list, to verify whether the self-hosted addresses of the originator or the beneficiary are under their control. By analogy with what was said before, it is believed that some of the solutions or measures outlined in the draft guidelines (such as advanced analytical tools) need further elaboration and may not guarantee an effective outcome in ascertaining whether the self-hosted address is owned or controlled by the originator or beneficiary. Furthermore, the rationale behind the requirement to use at least two solutions or measures is not clear. Effective risk mitigation could be achieved by using a single solution currently on the market for this purpose, provided that such technical solution is designed for the intended purpose of the draft guidelines, such as the so-called Satoshi test or the signing of an on-chain encrypted message sent to the self-hosted address. It is suggested that effective risk mitigation can be achieved even if a CASP has verified the ownership of the self-hosted address using only one of the methods that are aimed at fulfilling the guidelines requirement.

Guideline 72 addresses transfer of crypto-assets above 1000 EUR occurring between addresses hosted by CASP and self-hosted addresses where the self-hosted address is owned or controlled by a third person instead of the CASP customer. In these specific cases, in addition to the double verification required by draft guideline 69, CASPs are required to apply further enhanced verification measures, such as verifying the identity also through blockchain analysis solutions or third-party or public databases. In addition to what was said in the previous point about the redundancy of two methods for verifying the ownership of self-hosted addresses and the ineffectiveness for that purpose of some tools (blockchain analytics and third-party data providers), we consider it important to underline that achieving effective or immediate verification of the identity of the holder of a self-hosted address, through two solutions among those indicated in the draft guideline 69, is considered particularly challenging – from an

operational and technical standpoints – especially when the owner or the entity controlling it has not been previously identified or known by the CASP. In fact, if such a double check is already complex in the case of transfers with self-hosted addresses controlled by CASP customers, it is even more complex in the case of self-hosted addresses controlled by persons not previously identified by CASP.

9. Obligations on the payer's PSP, payee's PSP and IPSPs where a transfer is a direct debit

We appreciate these new guidelines that address the issue related to how to apply Regulation (EU) 2023/1113 in an SDD context.

However, these few amendments are suggested to fully clarify the matter:

- para. 75 – "*Where a transfer of funds is a direct debit, the PSP of the payee should send the required information on the payee to the PSP of the payer at the time when the direct debit* ***collection is sent.*** ~~*mandate is established or modified*~~*. Upon receipt of that information by the payer's PSP, the payee's PSP and IPSP should consider the information requirements in Article 4 points (2) and (4) and Article 5 points (1) and (2) of Regulation (EU) 2023/1113 to be met".*

- Para. 76 - For the purpose of paragraph 75:

  c) verification in Article 4(4) of Regulation (EU) 2023/1113 should be carried out by the PSP of the payee on the information of the payee, before sending the direct debit collection ***and derogation set out in paragraph (5) applies****;*

  d) verification in Article 7(3) and 7(4) of Regulation (EU) 2023/1113 should be carried out by the PSP of the payer (debtor PSP) on the information of the payer before debiting the payer's account ***and derogation set out in paragraph 7 (5) applies****.*