**Subject: EBA Consultation Paper EBA/CP/2023/35 on The Travel Rule Guidelines – discussion paper**

**Date:** 26/02/2024

---

The EBA is consulting on its draft new Travel Rule Guidelines:

The consultation paper only asks one question:

*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 maintained as drafted.*

Below are the main issues the EMA wishes to raise in response to the consultation question.

## EMA main issues

### 1. Maintaining a risk-based approach

The following statement in **para. 5 of the previous guidelines** has been omitted from the new guidelines:

> *5. The factors and measures described in these guidelines are not exhaustive. PSPs and IPSPs should consider other factors and measures as appropriate.*

This statement provided context for the guidelines, situating them within a risk-based approach to AML/CTF. Equally, the statement served to put firms on notice that they could not rely on the guidelines alone to discharge their obligations under the FTR. We think both these senses are important and recommend that the statement is re-instated.

### 2. Exemption for instruments used exclusively for the payment of goods and services

The process set out in **paras 4 and 5 of the draft guidelines** for assessing whether a card, e-money instrument or e-money token is used exclusively for the payment of goods and services risks counteracting the exemption by imposing onerous real-time per-transaction monitoring requirements on issuers.

For dual-use products that can be used to either make person-to-person transfers or purchases, a customer declaration of the purpose of the transfer ought to be sufficient, with ex-post monitoring in line with paras 4 and 5 a-c in place to assess the verity of declarations.

For single use products whose terms of use do not allow for person-to-person transfers, the exemption should be engaged in principle and issuers should merely be required to monitor ex-post for non-compliance with the terms in line with paras 4 and 5 a-c, making product level changes to restrict use to purchase transactions where required.

### 3. Identification of linked transfers

It is unclear to what purpose the definition of a linked transaction in **para. 7 of the draft guidelines** has been expanded by reference to persons linked with the payer or payee and to transaction that are '*sent from one payer to different payees or different payers to the same payee or persons connected with them within a short timeframe*.' These appear to be examples of money laundering typologies rather than of a set of transactions that together would amount to one transaction whose value exceeds a specified threshold. Given the importance of the understanding of linked transactions not only in the context of the FTR but across a range of AML laws and guidance, we suggest retaining the text in **para. 16 of the previous guidelines**.

### 4. Transition period

We welcome the transition period introduced in **para. 13 of the draft guidelines**. However, we believe this period should also be extended to PSPs in relation to transfers of crypto-assets, including asset-referenced-tokens (ARTs) or e-money tokens (EMTs). For example, e-money institutions issuing EMTs will need to comply with the new rules under the recast FTR for EMT transfers, in which case they should also be able to benefit from the transition period that applies to CASPs.

### 5. Choice of protocols

**Para. 15 of the draft guidelines** requires that CASPs ensure that information transmission protocols are sufficiently robust, seamless and interoperable. While we agree that these characteristics are desirable, CASPs do not have sufficient control over the availability of protocols, which are operated by third parties, to warrant a requirement of this type. Even where such protocols exist, CASPs cannot control their adoption by counterparty CASPs. We therefore suggest rephrasing this paragraph to require CASPs to take into account these characteristics when choosing a protocol rather than to ensure that protocols comply with these characteristics.

### 6. Multi-intermediation and cross-border transfers

**Para. 16 of the draft guidelines** requires PSPs and IPSPs to describe in their policy documentation how the required information is transmitted throughout the transfer chain. While there will be instances where the payment chain is under the control of, or at least fully visible to, the PSP/IPSP, there will also be many instances where this is not the case, particular for cross-

border transfers. The risk is that the guidelines favour PSPs that are part of a single system or scheme over independent PSPs. Therefore, the requirement here should be qualified through the wording 'where possible'.

Two issues arise in relation to **para. 17 of the draft guidelines**:

- The circumstances intended here, in which a PSP or IPSP does not have a direct relationship with the payer, are unclear and should be described in more detail (i.e., when does a PSP *not* have a direct relationship with the payer, and when *does* an IPSP have a direct relationship with the payer?) If by 'direct relationship' is meant 'business relationship', this should be clarified.
- Has the new requirement that the PSP must ensure that the next PSP in the transfer chain 'receives' the required information been intended? This would add an additional requirement to the legal requirement under the FTR, which is to merely *send* the required information. It should be noted that PSPs are not in a position to ensure that information is actually received by the next PSP in the transfer chain.

**Para. 18 of the draft guidelines** is superfluous. Every transfer may include a number of sub-transfers that may be settled through various accounts and arrangements, which can rightly be considered to constitute the movement of liquidity. This does not affect the transfer as a matter of law reflected in a change in the balances held by the payer and payee, which occurs independently from the value transfer and to which the requirements of the FTR relate.

## 7. Execution of transfers with missing information

Articles 8, 12, 17 and 21 of the recast FTR give PSPs and CASPs of payees/beneficiaries, as well as IPSPs and ICASPs a risk-based range of options for actions where information on a transfer is defective. This range is not reflected in **para. 50 of the draft guidelines**, which suggests that the execution of such a transfer is no longer an option where the originator or the beneficiary cannot be unambiguously identified due to missing or incomplete information. At least in relation to PSPs and CASPs of payees/beneficiaries and IPSPs and ICASPs, this paragraph therefore contradicts the legislative text and is not consistent with a risk-based approach.

Furthermore, it is unclear what 'unambiguously identified' would mean in practice. Where the relevant fields are completed with admissible information, this should meet the compliance threshold regardless of whether this information *in fact* identifies a single person unambiguously.

## 8. Verification of identity

**Para. 22 of the draft guidelines** requires PSPs and CASPs to verify the name of natural persons on the basis of 'an official and government-issued document (such as an identity card or passport).' This goes beyond the text of the recast FTR, which uses the phrase '*on the basis of*

*documents, data or information obtained from a reliable and independent source'* throughout when referring to verification requirements. It would be helpful if verification requirements could allow for some flexibility in relation to evidence, as customers wishing to initiate a transfer may not always have their government-issued ID to hand. In any case, guidance should not pre-empt any level 2 concessions that may be made in relation to acceptable evidence under the new AMLRs.

**Paras. 67 and 72 of the draft guidelines** appear to require CASPs to verify not just the identity of their own customer when sending to or receiving cryptoassets from an unhosted wallet, but also use '*cross-match data, including blockchain analytics and third-party data providers*' (para. 67) and the means in para. 72a-d for identifying or verifying the holder of the unhosted wallet to which their customer is transferring or from which they are receiving cryptoassets. This is not required by the text of Articles 14 and 16 of the recast FTR, which require CASPs only to verify the identity of their own customers.

While the recast FTR amends 4MLD to insert a new Article 19a under which the identification and verification of unhosted wallet holders may be required, Article 19a leaves it to firms to assess whether identification and verification is the appropriate risk-based measure to apply out of the four listed measures (Article 19a merely requires the choice of one measure). Furthermore, even where identification and verification are chosen, this is risk-based and may thus not be required in all cases.

Furthermore, the types of analysis referred to in paras. 67 and 72 typically relate to verifying the ownership/control of the unhosted wallet rather than the holder's identity. As such, they are misplaced here, as the verification of ownership is not required up to EUR 1,000 and is addressed by para. 69 of the draft guidelines.

Finally, it should be noted that the Article 19a requirements do not specify whether the self-hosted wallet is held by the CASP's customer or a third party. They should therefore be regarded as applying to both, not only to third parties, as stated in para. 72 of the draft guidelines.

**Para. 69 of the draft guidelines** sets out a list of measures for verifying the ownership/control of unhosted wallets, of which CASPs must use at least two. This prescriptive list exceeds what the FTR requires, which is merely 'adequate' (i.e., risk-based) measures. It is also unclear why two of the measures must be chosen, given that any one of them may establish control. For example, the same control over a self-hosted wallet is needed to sign a message or to send a small amount of crypto-assets, and adding both of them will not improve the quality of the verification, while increasing the duration of the process and decreasing the user experience of the CASP client. This is particularly pertinent given that some of the measures (e.g., attended verification) are too costly to constitute realistic options in the cryptoasset context.