

Response to the [Consultation Paper](#):
Guidelines on preventing the abuse of funds and certain
crypto-assets transfers for money laundering and terrorist
financing purposes under [Regulation \(EU\) 2023/1113](#)

By

21 ANALYTICS
CRYSTAL BLOCKCHAIN
EU BLOCKCHAIN OBSERVATORY & FORUM
EUROPEAN CRYPTO INITIATIVE
ROTATIONAL LABS
VASP HOLDINGS

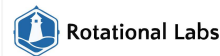
& Zornitsa Daskalova, Global Head of Financial Crime at Optima Partners

 21 ANALYTICS

 Crystal

 EUBlockchain

 euci
European Crypto Initiative

 Rotational Labs

 vasp
HOLDINGS

Introduction

We appreciate the opportunity to provide feedback on the Guidelines for preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under Regulation (EU) 2023/1113 (“EBA Travel Rule Guidelines”).

In general, the consultation document could benefit from more clear definitions and explanations of terms. A few practical examples of how the guidelines should be implemented by those expected to be affected could also offer improved comprehension and compliance.

Below, we make the suggestions to Section 4 (Preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes).

Our comments & Suggestions

Item 7: (1) It would be useful to add a definition of “short timeframe”. (2) Linked transfers in the context of crypto asset transfers are not mentioned in the Regulation or the Guidelines. It would be beneficial to clarify if and how these should be taken into account for the EUR 1000 threshold for self-hosted wallet ownership verification.

Item 10: We would like to address that, in practice, infrastructures and services that are devoid of any technical limitations do not exist. For the guidelines to be practical and realistic, the phrase "without the need to resolve technical limitations" ought to be replaced with "while being prepared to address any technical limitations that may emerge". Perhaps what is intended with this item is that CASPs only allow incoming and outgoing transactions after guaranteeing the system is fully capable of transmitting and receiving the information required under the Regulation, in which case it should be reworded for clarity.

Item 15: First, it is worth differentiating a *protocol* from a *technical solution*. The former is a set of rules for formatting and exchanging data so that all parties can process it. The latter - typically a paid-for vendor solution - can enable communication through the use of a single Travel Rule protocol, several, or none - in the case of CASPs using just email, for instance.

Although interoperability is an important and necessary feature, we believe this guideline conflates a commercial solution with a protocol. The most important thing for compliance is that CASPs guarantee they are reachable to their desired counterparties. Otherwise, according to the Regulation, they will not be able to transact.

However, commercial solutions will often not offer the flexibility required, as CASPs are only reachable by other paying members of that solution, and that solution may be restricted to a specific geographical region. In addition, they offer different features and requirements, on top of the communication technology, that appeals to different CASP's business models and regional regulations. Hence, unlike SWIFT for wire transfers, there is not a one-size-fits-all solution resulting in a global interoperable network.

On the other hand, open-source protocols give CASPs the flexibility required by their unique business model and requirements to interoperate with counterparties with other regional requirements to become compliant. Through the use of protocols that are vendor-neutral, and based on open standards and security best practices, CASPs can achieve maximum interoperability.

In the one and only recent case where [interoperability between Travel Rule protocols was achieved](#), it was done in the form of bridging software (which is in line with Item 11 of the Guidelines). That software speaks both Travel Rule Protocol (TRP) and the Travel Rule

Information Sharing Alliance (TRISA) protocol and translates between them. This is only possible because TRISA and TRP are open-source protocols, allowing developers and CASPs to inspect how their data is handled, and be able to work in a joint effort.

It is also unclear what “data integration” and “data reliability” means. We suggest aligning sub-item c with the Regulation's Recitals 19, 43 and 54.

Hence, we would suggest simplifying the wording in this guideline to:

"When choosing a technical solution for the Travel Rule, CASPs and ICASPs should ensure that the product or service can securely and seamlessly transmit the required information by:

- a. evaluating the solution's ability to be interoperable with the CASP's counterparties;
- b. considering its compatibility with industry standards, protocols, and blockchain networks involved; and
- c. assessing data processing, availability, and deletion."

Item 34: We would like to stress that no evidence was presented suggesting that self-hosted wallets are inherently riskier. We suggest aligning the requirements under the Guidelines with those under the Regulation (Recital 45) by adding the following wording to point E: “transfers with entities based in a third country that does not have licencing regimes or does not regulate PSP/CASP activity, or with self-hosted addresses **in the event that the crypto-asset service provider is or becomes aware that the information on the originator or beneficiary using the self-hosted address is inaccurate, or where the crypto-asset service provider encounters unusual or suspicious patterns of transactions.**”

If CASPs are expected to know the licensing and Travel Rule status of third-countries, it would be beneficial to call attention to it as part of their counterparty due diligence obligations. Currently, there is not a public list of jurisdictions where Travel Rule regulation has been implemented, although the FATF has shared as of mid-2023 that only 35 of its member countries (from 135 jurisdictions) had already passed legislation putting in place the Travel Rule. Therefore, the global regulatory status is heavily dynamic, which adds complexities for CASPs and ICASPs required to keep updated. If CASPs are required to onboard and complete due diligence on their counterparties, which would lead to knowing their counterparties' Travel Rule status, this should be made explicit.

Furthermore, "anonymity-enhancing techniques, products, or services" does not represent a unified category, but a spectrum of techniques, products, and services, only a segment of which represents ML/TF risk-increasing factors. On the contrary, a category of such tools, called privacy-enhancing technologies (or PETs), have been explored by privacy and compliance professionals as a possible solution to privacy issues in the context of AML compliance. Therefore, we ask that the Guidelines provide a finite list of high-risk techniques, products, or services based on their real risk factor.

In addition, there may be instances where a Crypto Asset Service Provider has supplied a comprehensive set of information, yet inaccuracies or errors are detected. When CASPs systematically provide inaccurate information, there are substantial risks. Inaccurate data can lead to misinterpretation, potentially impacting risk assessments, due diligence procedures, and overall compliance efforts. In such instances, it is crucial for the CASPs to acknowledge the error promptly, rectify the information, and implement mitigation measures to prevent recurrence.

Item 42: When CASPs are unable to safely return funds despite their best efforts, it is essential to define the steps to be taken, and how these funds should be handled. Possible actions and considerations that could be addressed in the guidance include: documentation and record-keeping requirements, escalation procedures, and risk mitigation measures.

It is relevant to note that it is technically possible to allow the actual transfer of crypto assets only after the transfer of Travel Rule data has been completed and agreed upon by both sides. This can mitigate the risk of receiving unacceptable funds from obliged entities. Currently, the only open protocol offering such a feature is the Travel Rule Protocol (TRP). This method may be the only workable technical way of addressing and guaranteeing compliance with Article 14(8) and Article 16 (3) while offering a communication channel for Article 17.

Item 65: Determining whether the beneficiary or originator's DLT address is with a CASP or with a self-hosted wallet is the key first step to compliance with Articles 14 and 16. It is important to note that wrongful identification of the type of address may lead to non-compliance with the Regulation since a transfer of crypto assets to an address wrongfully identified as a self-hosted wallet could be completed with the collection of, but without the exchange, of beneficiary and originator data. Likewise, an incoming transaction from a counterparty CASP that does not send the required data could go unidentified if the customer incorrectly self-reports ownership of the address.

The text mentions three (not exclusive) ways of determining whether a CASP is dealing with another CASP or self-hosted wallet. Although blockchain analytics can identify the counterparty based on DLT addresses, new wallets are easily created, which may lead to false attribution of the wallet type (hosted or self-hosted wallet) due to the lack of historical transaction information of newly created addresses. In fact, the majority of the crypto wallets avoid address reuse by default, for protecting on-chain information from being unmasked or tied to identities by unwanted parties.

Therefore, it is crucial that the guidelines clarify if CASPs are required to unequivocally determine the type of wallet prior to completion of the transaction, or if relying on customer's self-reporting, and blockchain analytics vendor probabilistic assessments is good enough.

It is unclear what "third-party data providers" and "identifiers used by messaging systems" mean, so these terms would benefit from clarification. However, it is also unlikely that either provides

identity data, as the only known available ways to tie a person's identity to a DLT address are the technical means cited in Item 69. A suggestion on how this section could be improved: "For the purposes of article 14(5) and Article 16(2), to determine whether the beneficiary or originator is using a CASP or a self-hosted address, the originator's CASP and the beneficiary's CASP should rely on a risk-based approach, leveraging available technical means as provided by the solution(s) the CASP uses and/or collect the information from the user, demanding cryptographic proof in case of claimed ownership."

Item 67: Identifying or verifying the identity of the originator or the beneficiary for a self-hosted address, after suitable technical means (see Item 69) establishing ownership/control of the crypto asset address, is separate from the information typically provided by blockchain analytics. Identifying or verifying the real world identity of a person, is the domain of eID solutions and related third-party providers. This distinction should be made clear in the Guidelines.

Item 69: First, there is no definition of the item "advanced analytical tools", which is a broad and unclear term. It would be beneficial to have an additional explanation, including what objectively constitutes a successful proof of ownership when using this method.

Sub-items "e. signing of a specific message in the account and wallet software, which can be done through the key associated with the transfer;" and "f. requesting the customer to digitally sign a specific message into the account and wallet software with the key corresponding to that address;" seem to be referring to the same technical mean. We would suggest deleting item e and rewording to keep item f as "requesting a verified/onboarded/logged-in customer to digitally sign a specific message with the private key corresponding to that address".

Additionally, the listed methods offer different levels of robustness. For instance, the level of confidence in their customer's proof of ownership over an address after receiving a message, signed with the address' private key, from a customer logged in the CASP's platform is highly different from a performed unattended verification. It is unclear why any CASP would need further verification steps after requesting a customer to perform the former since no additional or relevant information will be collected.

Item 72: In the case where a self-hosted wallet is not under the control of the direct customer (ownership/control could not be established as per Item 69), but there has been a collection of the required information (and the transfer of crypto-assets can be individually identified) this item in the Guidelines indicates that a risk-based approach can be taken.

The reference to Article 19a of Directive (EU) 2015/849 indicates that a self-hosted wallet identified as belonging to an entity in a third country requires additional due diligence as per Item 34 to ensure it is not in a country associated with high ML/TF risk.

But, if the additional data verification process does not identify that the self-hosted wallet belongs to a specific entity, a risk-based approach to the transaction should be taken. Factors could include transaction history, source of funds, and the relationship between the customer and the third-party wallet owner.

We advocate for an Enhanced Due Diligence (EDD) framework that is proportional and ensures fairness, avoiding the imposition of unnecessary obstacles for legitimate businesses in the cryptocurrency sector. Please clarify in the Guidelines this is an acceptable risk-based approach.

Item 73: Clarification should be provided in the guidelines, as the fact that a transfer involves a self-hosted address alone is not grounds for Enhanced Due Diligence (EDD).

Self-hosted wallets empower users to maintain control over their crypto-assets and mitigate the risks associated with relying on third parties. Self-hosted wallets primarily should not be the trigger for EDD, but as one risk-increasing factor as part of a risk-based approach. There exists a clear difference between the use of self-hosted wallets, and the use of techniques such as mixers or tumblers, or other tools tailored to obscure transactions. Unlike such tools or techniques, self-hosted wallets do not offer anonymity or transparency obfuscation, thus, transfers with them do not warrant Enhanced Due Diligence by default. AML due diligence relies on the nature of the financial activity itself rather than the specific technology utilised to execute the transaction.

It has to be noted that the UK Government's position on self-hosted wallets (June 2022 Consultation by HM Treasury) for example supports this approach:

"The government does not agree that unhosted wallet transactions should automatically be viewed as higher risk; many persons who hold cryptoassets for legitimate purposes use unhosted wallets due to their customizability and potential security advantages (e.g., cold wallet storage), and there is no good evidence that unhosted wallets present a disproportionate risk of being used in illicit finance".

Finally, to ensure coherence and clarity, we propose a unification and clarification of the terms in Articles 67, 69, and 72, specifically concerning the phrases "blockchain analytics", "advanced analytical tools," and "blockchain analytic data." This is essential for a more precise interpretation and implementation of the specified articles.

We commend the EBA for issuing these guidelines, highlighting several challenges and how CASPs should address them. We thank the EBA for the opportunity to respond to the consultation and look forward to the finalised guidelines.

Sincerely,

Response to the [Consultation Paper](#): Guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under [Regulation \(EU\) 2023/1113](#)

21 ANALYTICS
CRYSTAL BLOCKCHAIN
EU BLOCKCHAIN OBSERVATORY & FORUM
EUROPEAN CRYPTO INITIATIVE
ROTATIONAL LABS
VASP HOLDINGS

& Zornitsa Daskalova, Global Head of Financial Crime at Optima Partners

