February 26, 2024

European Banking Authority

Delivered via: Consultation submission portal

Re: Consultation on the Guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under Regulation (EU) 2023/1113

Notabene Inc. welcomes the opportunity to comment on the European Banking Authority's ("**EBA**") consultation on the "Guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under Regulation (EU) 2023/1113" ("**EBA Guidelines**"). We applaud the EBA in its aims to promote the development of a common understanding by PSPs, IPSPs, CASPs and ICASPs, and competent authorities across the EU and how they should be applied. We welcome the opportunity to be part of the ongoing dialogue and are available for follow-up meetings regarding our responses.

Introduction and Overview:

Notabene, the crypto industry's only pre-transaction authorization decision making platform, helps to identify and stop high-risk activity before it occurs. The platform offers a secure, holistic view of crypto transactions, enabling customers to automate real-time decision-making, perform counterparty sanctions screening, identify self-hosted wallets, conduct VASP Due Diligence, and complete the smooth rollout of Travel Rule compliance in line with global regulations.

Notabene was founded in 2020 with the explicit mission to enable safe and trusted crypto transactions by developing a comprehensive solution to help companies comply with the FATF's Travel Rule. A continued strong relationship with global financial regulators, including FATF, industry associations, and Virtual Asset Service Providers (VASPs) across multiple jurisdictions, arms us with an unparalleled view of the complex and critical nature of regulatory compliance in the crypto space.

It is worth pointing out that, even with current AML and know-your-customer (KYC) compliance frameworks in place, VASPs can unknowingly facilitate transactions with sanctioned counterparties. **Only Travel Rule compliance gives VASPs transaction-level counterparty and sanction insight, allowing them to recognize if their clients are sending transactions to sanctioned entities, wallets, or jurisdictions.** VASPs worldwide are in different stages of compliance, which leaves many companies vulnerable to exposure to sanctioned individuals.

We appreciate the opportunity to respond to this consultation and look forward to continued engagement and clarification.

Very truly yours,

Lana Schwartzman
Head of Regulatory and Compliance

Catarina dos Santos Veloso

Catarina Veloso
Regulatory and Compliance Senior Associate

RESPONSE TO CONSULTATION

Introduction **4**
Application timeline **4**
Notabene’s Request/Recommendation 5
Self-hosted wallets **6**
Transactions not exceeding 1,000 Euros 6
Notabene’s Request/Recommendation 7
First-party transactions exceeding 1,000 Euros 8
Notabene’s Request/Recommendation 9
Third-party transactions exceeding 1,000 Euros 11
Notabene’s Request/Recommendation 12
Non-compliant deposits **14**
Notabene’s Request/Recommendation 15
Interoperability **17**
Notabene’s Request/Recommendation 18

Introduction

Given Notabene's focus and extensive experience in crypto Travel Rule compliance, our response to the consultation will focus on the provisions of the EBA Guidelines that apply to CASPs.

Where appropriate, our response includes:

- Transcriptions of relevant provisions of Regulation (EU) 2023/1113 of the European Parliament and of the Council ("TFR") and of the EBA Guidelines to facilitate the joint reading and interpretation of the regimes set forth therein;
- Suggested changes to the current drafting of the EBA Guidelines, with the goal of accurately conveying our policy proposals (suggested deletions are identified in **~~red~~** and suggested additions are identified in **green**).

Throughout the document we use "CASPs" to refer to EU crypto-asset providers as defined in the TFR and "VASPs" to more broadly refer to entities of equivalent nature globally.

Application timeline

Following ESMA's communication from October 2023, it came to our attention that there are different interpretations of the relationship between the grandfathering clause set in Regulation (EU) 2023/1114 of the European Parliament and of the Council ("MiCA") and the entry into force of the TFR.

On one hand, according to the MiCA grandfathering clause, Member States may allow CASPs in their jurisdiction to continue providing services without a MiCA license until **July 1, 2026**. On the other hand, according to the TFR, Travel Rule obligations therein apply from **December 30, 2024**.

Our interpretation is that the transitional regimes are independent - therefore, even if the CASP can operate without a MiCA license until July 1, 2026, it must comply with the requirements of the TFR as of December 30, 2024.

However, we became aware of a conflicting interpretation that conditions the applicability of the TFR to the grandfathering period allowed in each member state (i.e., if the grandfathering period is until July 1, 2026, the TFR would only apply from that moment on).

Still, on the timeline of application, paragraph 13 of the EBA guidelines foresees a transitional period until **July 31, 2025**, during which CASPs may exceptionally use infrastructures or services that are not fully capable of transmitting the required information, provided that they put in place additional policies and procedures to compensate for technical limitations.

In our view, this does not exempt CASPs from complying with Travel Rule obligations until 31 July 2025 in any way, but we have also become aware of interpretations in this direction.

Notabene's Request/Recommendation

While being aware that any unclarity on the application timeline does not stem from the EBA or its Guidelines, we kindly request that the EBA provides clarity on both raised issues in the final text of the Travel Rule guideline, as this would help alleviate confusion that may hinder a smooth roll out of requirements within the EU.

Self-hosted wallets

Transactions not exceeding 1,000 Euros

TFR	**EBA Guidelines**
14.5. 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. 16.2. In the case of a transfer of crypto-assets made from a self-hosted address, the crypto-asset service provider of the beneficiary **shall obtain and hold the information referred to in Article 14(1) and (2)** and shall ensure that the transfer of crypto-assets can be individually identified.	67. Where the crypto-asset transfer is not made from or to another CASP or any other obliged entity, but from or to a self-hosted address, in order to obtain the required information on the originator or beneficiary, the beneficiary's CASP and originator's CASP respectively, should collect the information from their customer. The beneficiary's CASP and originator's CASP should 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.

According to Articles 14/5 and 16/2 of the TFR, **in crypto asset transfers to or from self-hosted wallets not exceeding 1,000 Euros** the originator CASP and beneficiary CASP, respectively, are required to **obtain and hold** the information about the originator and beneficiary customers specified in paragraphs 1 and 2 of Article 14.

However, paragraph 67 of the EBA Guidelines provides that **in crypto asset transfers to or from self-hosted wallets not exceeding 1,000 Euros**[1] CASPs should:

- Collect the required information from their customer; and
- "*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***".

This requirement to verify the identity of the originator or beneficiary in transactions with self-hosted wallets not exceeding 1,000 EUR introduces a stricter framework than the one that results from the TFR. The TFR distinguishes the requirements that apply to transactions between CASPs and self-hosted wallets based on transaction amount, with the intention of enforcing obligations proportional to the transaction risk. In our view, the requirement introduced in the second sentence of paragraph 67 of the EBA Guidelines undermines the proportionality of the requirements

[1] Paragraph 67 does not explicitly state that it applies to crypto asset transfers to or from self-hosted wallets not exceeding 1,000 Euros. This is inferred from the structure of the EBA Guidelines, considering that the subsequent section (8.2.3) applies to self-hosted wallet transfers above 1,000 Euros.

applicable to transactions with self-hosted wallets not exceeding 1000 Euros that the TFR intended to achieve.

Additionally, the identity of the originator or beneficiary cannot be verified by cross-matching data with blockchain analytics, as these providers have no information that binds a person's identity with a specific wallet address. We are not aware of other third-party providers with wide adoption that could assist in this process. Hence, in addition to undermining proportionality, the requirement introduced in the second sentence of paragraph 67 of the EBA Guidelines does not appear technically feasible to implement.

Notabene's Request/Recommendation

Notabene humbly proposes that this requirement be removed and that, instead, CASPs are encouraged to assess the transaction risk (for example, by screening the available information against blockchain analytics and sanction screening providers) and decide whether or not to proceed with the transaction based on their risk assessment.

Proposed drafting:

*67. Where the crypto-asset transfer is not made from or to another CASP or any other obliged entity, but from or to a self-hosted address, in order to obtain the required information on the originator or beneficiary, the beneficiary's CASP and originator's CASP respectively, should collect the information from their customer. The beneficiary's CASP and originator's CASP should use suitable technical means****, including blockchain analytics and sanction screening providers, for the purpose of assessing the risk of the transaction before authorizing it****.*

First-party transactions exceeding 1,000 Euros

TFR	EBA Guidelines
14.5. Without prejudice to specific risk mitigating measures taken in accordance with Article 19b of Directive (EU) 2015/849, in the case of a transfer of an amount exceeding EUR 1 000 to a self-hosted address, **the crypto-asset service provider of the originator shall take adequate measures to assess whether that address is owned or controlled by the originator**. 16.2. Without prejudice to specific risk mitigating measures taken in accordance with Article 19b of Directive (EU) 2015/849, in the case of a transfer of an amount exceeding EUR 1 000 from a self-hosted address, **the crypto-asset service provider of the beneficiary shall take adequate measures to assess whether that address is owned or controlled by the beneficiary**.	68. For the purpose of assessing whether the self-hosted address in transfers above 1 000 EUR is owned or controlled by the CASP's customer, as referred to in Article 14(5) and Article 16(2) of Regulation (EU) 2023/1113, the CASPs should use the exchange rate of the crypto-asset being transferred to determine its value in euros at the time of the transfer. 69. Where the amount of a transfer from or to a self-hosted address exceeds 1 000 EUR, the originator's CASP and beneficiary's CASP should verify whether the self-hosted address is owned or controlled by the originator and beneficiary, respectively, by using suitable technical means, **which include at least two of the following**: a. advanced analytical tools; b. unattended verifications as specified in the ''Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849''15 displaying the address; c. attended verification as specified in the ''Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849''; d. sending of a predefined amount (preferably the smallest denomination of a given crypto-asset), set by the CASP, from and to the self-hosted address to the CASP's account; e. signing of a specific message in the account and wallet software, which can be done through the key associated with the transfer; f. requesting the customer to digitally sign a specific message into the account and wallet software with the key corresponding to that address; g. other suitable technical means as long as they allow for reliable and secure assessment and the CASP is fully satisfied that it knows who owns or controls the address. 70. The decision on which method(s) to choose should depend on: a. the technical capabilities of the self-hosted address; and b. the robustness of the assessment each method can deliver. 71. Where two methods on their own are not sufficiently reliable to ascertain the ownership or controllership of a self-hosted address, the CASP should ensure that a combination of more methods is used.

According to Articles 14/5 and 16/2 of the TFR, **in crypto asset transfers to or from self-hosted wallets exceeding 1,000 Euros** the originator CASP and beneficiary CASP, respectively, are required to **take adequate measures to assess whether the wallet is owned or controlled by its customer** (i.e., the originator CASP must assess whether the wallet is owned or controlled by the originator, and the beneficiary CASP must assess whether the wallet is owned or controlled by the beneficiary).

In these cases, paragraph 69 of the EBA Guidelines **requires that CASPs use at least two suitable technical means to** conduct the control or ownership verification

(“[...]*the originator’s CASP and beneficiary’s CASP should verify whether the self-hosted address is owned or controlled by the originator and beneficiary, respectively,* ***by using suitable technical means, which include at least two of the following***”[...]). Our interpretation of the current wording is that CASPs are required to **apply two methods of wallet ownership/control verification each time such verification is required**[2].

In our view, requiring two methods for verifying wallet ownership/control may not enhance the verification process and could lead to inefficient practices as well as force the adoption of potentially inefficient practices. For instance, if a customer proves access to a wallet's private keys by signing a cryptographic message, asking them to also send a specific amount from that wallet merely duplicates the effort to show control over the keys. This approach is similar to an overly redundant two-factor authentication, like asking a customer to click on a link sent to their email not once but twice.

Notabene’s Request/Recommendation

Notabene humbly proposes that CASPs are recommended to **use additional methods when (i) one method on its own is not sufficiently reliable** to ascertain the ownership or control of the self-hosted address, and (ii) the adoption of additional methods improves the degree of reliability of that verification.

Additionally, we recommend the clarification of the following aspects:

- **Timing for evaluation of transaction amount**: Paragraph 68 of the EBA guidelines determines that the value of the self-hosted wallet transaction in Euros should be assessed using the exchange rate ***at the time of the transfer***. However, if the obligations regarding transactions with self-hosted wallets are to be complied with **before authorizing the transaction**, the Euro value must be determined based on the exchange rate at the time the transaction is initiated rather than when it is executed.
- **Distinction between wallet ownership/control verification methods:** Paragraph 69 lists several methods that can be adopted to verify wallet ownership/control. It would be beneficial to clarify the distinction between method e. and f. (“[...] *e.* ***signing of a specific message*** *in the account and wallet software, which can be done through the key associated with the transfer; f. requesting the customer to* ***digitally sign a specific message*** *into*

[2] An alternative interpretation would be that CASPs need to set up at least two technical methods of wallet ownership / control verification, giving them enough flexibility to fulfill this requirement in different circumstances (e.g., the CASP could use one method when the customer’s wallet is with certain wallet providers, another method when the asset is transferred using a certain network, etc.). This is not what seems to result from the letter of the EBA Guidelines. If this is the regulatory intention, it should be made explicit.

the account and wallet software with the key corresponding to that address […]")

Proposed drafting:

68. For the purpose of assessing whether the self-hosted address in transfers above 1 000 EUR is owned or controlled by the CASP's customer, as referred to in Article 14(5) and Article 16(2) of Regulation (EU) 2023/1113, the CASPs should use the exchange rate of the crypto-asset being transferred to determine its value in euros at the time of the transfer **initiation**.

69. Where the amount of a transfer from or to a self-hosted address exceeds 1 000 EUR, the originator's CASP and beneficiary's CASP should verify whether the self-hosted address is owned or controlled by the originator and beneficiary, respectively, by using suitable technical means, **which include at least one of the following**: […]

71. Where **one method on its own** is not sufficiently reliable to ascertain the ownership or controllership of a self-hosted address, the CASP should ensure that a combination of more methods is used **if such improves the degree of reliability of the verification**.

Third-party transactions exceeding 1,000 Euros

EBA Guidelines	**Directive (EU) 2015/84916**
72. Where the self-hosted address is owned or controlled by a third person instead of the CASP customer, the CASP should, in addition to applying the verification requirement in accordance with Article 14 (5) or Article 16 (2) of Regulation (EU) 2023/1113, apply mitigating measures commensurate with the risks identified as per Article 19a of Directive (EU) 2015/84916. **Verification in this context is deemed to have taken place when the CASP collects additional data from other sources to verify the submitted information**, namely from: a. blockchain analytic data; b. third-party data; c. recognised authorities' data; or d. publicly available information, as long as those are reliable and independent.	Article 19a 1. Member States shall require crypto-asset service providers to identify and assess the risk of money laundering and terrorist financing associated with transfers of crypto-assets directed to or originating from a self-hosted address. [...] **Member States shall require crypto-asset service providers to apply mitigating measures commensurate with the risks identified. Those mitigating measures shall include one or more of the following:** (a) taking risk-based measures to identify, **and verify the identity of, the originator or beneficiary of a transfer made to or from a self-hosted address** or the beneficial owner of such originator or beneficiary, including through reliance on third parties; (b) requiring additional information on the origin and destination of the transferred crypto-assets; (c) conducting enhanced ongoing monitoring of those transactions; (d) any other measure to mitigate and manage the risks of money laundering and terrorist financing as well as the risk of non-implementation and evasion of targeted financial sanctions and proliferation financing-related targeted financial sanctions.

The TFR is silent on the obligations that apply to transactions exceeding 1,000 Euros with self-hosted wallets that do not belong to the CASP's customer, but do to a third-party. In paragraph 72, the EBA Guidelines introduce a framework that applies to these cases. According to this provision, in transactions exceeding 1,000 Euros with self-hosted wallets of third-parties, CASPs are required to:

- Apply the ***verification requirement*** in accordance with Article 14 (5) or Article 16 (2) of Regulation (EU) 2023/1113

  [i.e., "*the crypto-asset service provider of the originator shall take adequate measures to **assess whether that address is owned or controlled** by the originator.*" || "*the crypto-asset service provider of the beneficiary shall take adequate measures to **assess whether that address is owned or controlled** by the beneficiary.*"]

- Apply mitigating measures commensurate with the risks identified as per Article 19a of Directive (EU) 2015/84916

Further, paragraph 72 states that "***[v]erification*** *in this context is deemed to have taken place when the CASP collects additional data from other sources to verify the submitted information, namely from: […]*".

In our view, it is not clear what ***verification*** is deemed to have taken place by collecting data from the referred sources. As paragraph 72 mentions the "***verification requirement***" of TFR articles 14/5 and 16/2 of the TFR, one plausible interpretation is that the last sentence of paragraph 72 refers to the wallet ownership/control verification[3].

If this interpretation is correct, this would suggest that the **wallet ownership/control verification is deemed to have taken place by collecting additional data to verify the submitted information from sources like blockchain analytics, third-parties, recognized authorities or publicly available information**. However, we fail to see how these sources could be used to verify wallet ownership/control of a third party as blockchain analytics cannot link a person's identity with a specific wallet address, and we are not aware of other data sources with wide adoption that could assist in this process.

Notabene's Request/Recommendation

We humbly request that the regulatory intention regarding transactions exceeding 1,000 Euros between CASPs and third-party self-hosted wallets be clarified. This is especially important given that these cases are not covered in the TFR.

Regarding the desired treatment of transactions between CASPs and third-party self-hosted wallets, we would like to point out that when national Travel Rule frameworks require VASPs to verify the identity and/or wallet ownership/control of a third-party self-hosted wallet owner, VASPs often cannot meet this requirement at scale. Consequently, many VASPs address this limitation by simply restricting transactions with third-party self-hosted wallets due to the impracticality of reliably verifying the identity and control/ownership of the third-party owner of self-hosted wallets. Such an approach eventually leads customers to transfer funds to themselves before finally transferring those funds to the third-party beneficiary, which ultimately does not benefit the regulatory goal of increasing the traceability of transactions with self-hosted wallets.

In fact, according to the results of Notabene's 2024 State of Crypto Travel Rule Compliance Report[4], 33% of respondents **only allow first-party transactions** and

[3] Article 19a of Directive (EU) 2015/84916 also mentions a verification measure in 1/(a) - verifying the identity of the originator or beneficiary of the self-hosted address. However, this measure is only required if commensurate with the risks identified by the CASP. So it seems less likely that the last sentence of section 72 refers to this verification requirement.

[4] The corresponding survey report with the methodology will be published soon.

require their customers to demonstrate control over the wallet, whereas 6% opted to prohibit transactions with self-hosted wallets.

Hence, our proposal is that **in transactions with third-party self-hosted wallets, CASPs are required to apply mitigating measures commensurate with the risks identified as per Article 19a of Directive (EU) 2015/84916**. This allows CASPs to take a risk-based approach and apply the risk mitigation measures that are adequate to the transaction profile. To evaluate the risk of the transaction, CASPs should be encouraged to resort to additional information sources, such as blockchain analytics.

Proposed drafting:

72. Where the self-hosted address is owned or controlled by a third person instead of the CASP customer, the CASP should, ~~**in addition to applying the verification requirement in accordance with Article 14 (5) or Article 16 (2) of Regulation (EU) 2023/1113**~~, apply mitigating measures commensurate with the risks identified as per Article 19a of Directive (EU) 2015/84916. **To evaluate the risk of the transaction, the CASP shall collect additional data from other sources**, namely from blockchain analytic data a**nd, where available,** third-party data, recognized authorities' data or publicly available information, as long as those are reliable and independent.

Non-compliant deposits

TFR	EBA Guidelines
17.1. The crypto-asset service provider of the beneficiary shall implement effective risk-based procedures, including procedures based on the risk-sensitive basis referred to in Article 13 of Directive (EU) 2015/849, for **determining whether to execute, reject, return or suspend a transfer of crypto-assets lacking the required complete information on the originator and the beneficiary** and for taking the appropriate follow-up action.	40. The risk-based policies for determining whether to reject, suspend or execute a transfer in accordance with Article 8(1), Article 12, Article 17(1) and Article 21 should consider the ML/TF risk associated with that transfer before deciding on the appropriate course of action. 41. CASPs should consider in their assessment before deciding on the appropriate course of action whether or not: a. the information allows for determination of the subjects of the transfer; and b. one or more risk-increasing factors have been identified that may suggest that the transfer presents a high ML/TF risk or gives rise to suspicion of ML/TF (see Section 5.3). 49. **Where a CASP becomes aware that required information is missing**, incomplete or provided using inadmissible characters during the transfer **and executes the transfer, based on all relevant risks, and provided that the condition in paragraph 50 is not met**, it should document the reason for executing that transfer and, in line with its risk-based policies and procedures, consider the future treatment of the prior CASP or self-hosted address in the transfer chain for AML/ CFT compliance purposes. 50. **Where the originator or beneficiary cannot be unambiguously identified** due to missing or incomplete information, or information provided using inadmissible characters, **the CASP should not execute the transfer.**

According to Article 17/1 of the TFR, CASPs shall adopt risk-based procedures to determine whether to execute, reject, return, or suspend a transfer that lacks the required complete information on the Originator and Beneficiary. This clause allows CASPs the flexibility to execute transfers under such conditions, basing the decision on their risk assessment procedures instead of fixed criteria.

However, paragraphs 49 and 50 of the EBA Guidelines establish specific criteria for CASPs to execute transfers lacking complete information, irrespective of their risk assessment of the transaction. This criteria dictates that such transfers can only be executed if the received information, although incomplete, enables the **unambiguous identification of the parties to the transaction**.

By foreseeing the unambiguous identification of the parties as a mandatory criteria, **the EBA Guidelines introduce a stricter framework than that prescribed by the TFR** (which leaves the decision to execute, reject, return or suspend the transfer entirely subject to the risk procedures set by the CASP). This situation is problematic because due to the **sunrise period and interoperability limitations**—challenges that CASPs cannot address independently—there r**emains a significant percentage of transactions lacking the necessary Travel Rule information.** This means that in most cases, the issue that CASPs face is **not receiving any information at all**, rather than receiving incomplete information that may allow for unambiguous identification of the parties.

According to the results of Notabene's 2024 State of Crypto Travel Rule Compliance Report[5], **37% of respondents have never received a Travel Rule transfer**. It is worth noting that this percentage only includes respondents who have **never** received a travel rule transfer; **the percentage of respondents who have received travel rule transfers but still do not receive transfers for a substantial percentage of their deposits is expected to be much higher**.

This data demonstrates that requiring CASPs not to execute any transactions where the unambiguous identification of the parties is not possible will have a significant impact on CASPs' businesses (for 37% of respondents to our survey) and would entail rejecting or returning all deposits from counterparty VASPs.

Further, when required to reject or return funds due to missing or incomplete information, CASPs face additional hurdles. After the transaction is settled, it becomes extremely challenging to safely handle the return of funds as the process exposes CASPs to liability for loss of funds and sanction breaches. Beneficiary CASPs cannot assume that the funds received can be returned to the originating wallet address, as that address might not be prepared to receive funds and, therefore, funds could be lost. Additionally, by returning funds without a clear understanding of their origin, VASPs run the risk of sending funds back to sanctioned or high-risk actors.

Notabene's Request/Recommendation

Notabene humbly proposes that the standard set by the TFR be reinstated. CASPs should be allowed to execute the crypto asset transfer solely subject to their risk procedures, even if the received information does not allow for unambiguous identification of the parties. This standard could be revised, and the unambiguous identification of the parties could be reintroduced as a mandatory criteria at a later stage once evidence shows that CASPs are receiving Travel Rule with most deposits.

[5] The corresponding survey report with the methodology will be published soon.

Additionally, it would be beneficial to clarify the difference between "rejecting" and "returning" a transfer of crypto-assets (Would rejecting apply to cases where the CASP detects missing or incomplete information before receiving the funds, and therefore can "reject" receiving them? Would "returning" apply to all cases where non-compliance is detected post-settlement?).

Proposed drafting:

49. **Where a CASP becomes aware that required information is missing**, incomplete or provided using inadmissible characters during the transfer **and executes the transfer, based on all relevant risks**~~**, and provided that the condition in paragraph 50 is not met,**~~ it should document the reason for executing that transfer and, in line with its risk-based policies and procedures, consider the future treatment of the prior CASP or self-hosted address in the transfer chain for AML/ CFT compliance purposes.

~~50. **Where the originator or beneficiary cannot be unambiguously identified** due to missing or incomplete information, or information provided using inadmissible characters, **the CASP should not execute the transfer.**~~

Interoperability

EBA Guidelines
15. When choosing the messaging protocol, **CASPs and ICASPs should ensure that the protocol's architectures are sufficiently robust to enable the seamless and interoperable transmission of the required information** by: a. evaluating the protocol's **interoperability features to ensure it can seamlessly communicate with other systems**, both within and outside CASPs and ICASPs; b. considering the compatibility with existing industry standards, protocols, and blockchain networks to facilitate integration; and c. assessing data integration and data reliability.

Currently, the lack of interoperability between Travel Rule solutions continues to limit VASPs' ability to comply with the Travel Rule fully. Results from Notabene's 2024 State of Crypto Travel Rule Compliance Report[6] show that **interoperability between tools is the main hindrance to Travel Rule implementation, with 34% of respondents ranking it as their number one concern**. We applaud the EBA's mandate for CASPs to assess Travel Rule protocols' interoperability features, ensuring seamless communication with other systems. This is a crucial move to encourage the industry to adopt open and interoperable communication standards.

Regarding this aspect, it's important to note that current interoperability features remain below expectations. Efforts to achieve interoperability among Travel Rule protocols and solutions, aiming to dismantle compliance silos, are still facing significant challenges, primarily due to the use of proprietary Travel Rule protocols[7]:

- **Technical integration challenges**

  Integration with closed Travel Rule protocols requires access to proprietary technical information, which is often not granted for commercial and competitive reasons. Additionally, technical integration often requires collaboration from the protocols' team members, which may be hindered by conflicting priorities.

- **Membership in closed Travel Rule protocols**

  Achieving technical interoperability does not eliminate the need for securing membership in closed Travel Rule protocols. i.e., even if a CASP uses a solution that is technically interoperable with a closed Travel Rule protocol, the CASP will be unable to exchange information with its members unless they secure membership in that protocol.

  Access to membership is, in turn, subject to a centralized and discretionary due diligence process carried out at network level on each applicant VASP. On

[6] The corresponding survey report with the methodology will be published soon.

[7] Closed Travel Rule protocols are messaging protocols that work as closed networks, i.e., where VASPs can only adopt the protocol for sending and receiving Travel Rule messages to the members of the network and where access to the network is subject to a centralized and discretionary vetting process.

this matter, the FATF has clarified that the due diligence process should be conducted autonomously and independently by each VASP and that the need for network-level control of membership should not obstruct interoperability efforts. As reported by the FATF in its June 2023 Targeted Update, "*the rationale is that compliance tool providers may screen users of their tool to ensure adequate data protection controls or even a level of counterparty due diligence, and therefore consider that allowing information sharing only between tool users (i.e., no interoperability).*" However, the FATF clarified that "***VASPs are required to independently assess counterparty risk***" and that this approach from closed Travel Rule networks—"*does not remove the need for VASPs to independently verify the information and ensure all relevant domestic obligations are met.*".

Considering that all relevant closed Travel Rule protocols are operated by VASPs with significant market share also poses antitrust concerns. By controlling access to the protocol, the operators can also determine the competitors that are able to engage in compliant transaction flows.

- **Variations in Travel Rule workflows**

  The differences in Travel Rule workflows also hinder interoperability efforts.

  On one hand, some Travel Rule protocols implement flows that are not suitable to meet FATF standards, or the requirements now set in the TFR and proposed in the EBA Guidelines. In its June 2023 Targeted Update, the FATF reported that many Travel Rule compliance tools fall short of the FATF standards. A common shortfall is only facilitating the transmission of Travel Rule information *after* the on-chain crypto asset transfer and the coverage of a limited range of crypto assets.

  On the other hand, there are multiple ways of setting up Travel Rule–compliant workflows, which means that reconciliation issues often arise even when both protocols/solutions are technically compliant.

Due to these limitations, CASPs' assessment of Travel Rule solutions and protocols will often conclude that their interoperability features are very limited. This persistent lack of interoperability is beyond the control of CASPs and, frequently, of the Travel Rule solution itself - open and protocol-agnostic solutions encounter barriers in freely and proactively integrating with closed Travel Rule protocols due to the factors mentioned above.

Notabene's Request/Recommendation

Notabene humbly recommends that, in addition to evaluating the interoperability features, CASPs should consider the Travel Rule solution/protocol reachability metrics (i.e., the counterparties that can be reached using the solution and the rate of Travel Rule transfers that would successfully be sent to the intended beneficiary). Even though the Travel Rule solution/protocol may have limited interoperability with others due to factors beyond its control, as previously explained, this is expected to minimally impact CASPs' compliance capabilities, provided that the assessment of the reachability metrics yields positive outcomes.

Additionally, to emphasize the EBA Guidelines' role in encouraging the adoption of open and interoperable communication standards within the industry, CASPs evaluation of Travel Rule solutions/protocols should also consider the following factors:

- Does the Travel Rule solution/protocol empower the CASP to transmit information to any counterparty, subject to its own due diligence assessment?; or
- Does the adoption of the Travel Rule solution/protocol entail only being able to transmit information to counterparties accepted into the network through a centralized vetting process at network-level? (If so, the Travel Rule solutions/protocols should be deemed inadequate).

Proposed drafting:

15. When choosing the messaging protocol, **CASPs and ICASPs should ensure that the protocol's architectures are sufficiently robust to enable the seamless and interoperable transmission of the required information** by:

a. evaluating the protocol's **interoperability features to ensure it can seamlessly communicate with other systems**, both within and outside CASPs and ICASPs. **If the Travel Rule solution or protocol exhibits limited interoperability with closed Travel Rule protocols due to factors beyond its control, the CASP should evaluate its reachability metrics (i.e., the counterparties that can be reached using the protocol/solution and the rate of Travel Rule transfers that would successfully be sent to the intended beneficiary). Positive results from the assessment of reachability metrics would indicate the protocol/solution is suitable despite the limited interoperability features.**
b. evaluating if the protocol enables transmission of information to any counterparty, subject to the CASP's own due diligence assessment, rather than restricting transmission solely to counterparties accepted through a centralized network-level vetting process. If the protocol limits transmission in this way, it should in principle be considered inadequate.
c. considering the compatibility with existing industry standards, protocols, and blockchain networks to facilitate integration; and
d. assessing data integration and data reliability.

Finally, we suggest that the EBA provides guidance on how to evaluate the suitability of Travel Rule compliance tools on a more substantive level (e.g., the ability to support CASPs detecting deposits with missing or incomplete information and taking relevant action). Notably, the Hong Kong Securities and Futures Commission provides clear criteria for VASPs to determine whether the Travel Rule solution provider enables them to comply with Hong Kong Travel Rule requirements in an effective and efficient manner[8]. It would be beneficial for the EBA to adopt a similar approach, further supporting CASPs in assessing the suitability of Travel Rule compliance tools to comply with the requirements set in its Guidelines.

[8] HK SFC's AML/CTF Guideline for SFC-licensed VASPs 2023, pg. 169, paras. 12.12.2