coinbase

To:

European Banking Authority
Tour Europlaza
20 avenue André Prothin
CS 30154
92927 Paris La Défense CEDEX
France

Date:

26 February 2024

EBA Consultation on the Travel Rule Guidelines

Coinbase Global, Inc. and its EU subsidiary Coinbase Europe Limited (together, "Coinbase") welcome the opportunity to respond to the European Banking Authority's ("EBA") consultation on its proposed guidelines (the "Proposed Guidelines") regarding implementation of Regulation (EU) 2023/1113 (the "Travel Rule"). Specifically, the Proposed Guidelines aim to help payment service providers ("PSPs"), intermediary PSPs ("IPSPs"), crypto-asset service providers ("CASPs"), and intermediary CASPs ("ICASPS") comply with requirements to detect missing or incomplete information that accompanies a transfer of funds or crypto-assets pursuant to the Travel Rule.[1]

Coinbase fully supports effective regulation developed with the input and coordination of industry members. These discussions come at a time of enormous opportunity for Europe to lead the world in digital asset innovation, but this opportunity depends in significant part on the EBA creating a regulatory landscape that fosters the growth of compliant CASPs while holding accountable those that fail to meet their obligations. In this response, we provide feedback on certain parts of the Proposed Guidelines to help ensure that compliance with them achieves our shared goal of curbing illicit finance through broader adherence to the Travel Rule.

[1] For clarity, in this response "Travel Rule" refers to the relevant provisions within Regulation (EU) 2023/1113. Conversely, "travel rule" is used to refer more generally to similar regulations as they exist across many jurisdictions.

coinbase

Executive Summary

Coinbase recognises and appreciates the important work that the EBA has done in drafting these Proposed Guidelines. We are broadly supportive of the further clarity the Proposed Guidelines provide and the overarching objective of strengthening the EU's AML/CTF regimes particularly in connection with the transfer of funds and crypto assets, however we are highlighting four key areas that would present challenges and concerns for the industry, particularly around the treatment of self-hosted wallets ("SHWs"). We offer below a summary of our key points:

1. **The Proposed Guidelines should encourage CASPs to adopt Travel Rule compliance solutions that prioritize data privacy and security, robust counterparty due diligence reviews, and global coverage -** prioritising interoperability may result in lower security and privacy standards, which could otherwise be maintained and AML objectives delivered via solutions that offer global coverage.
2. **The Proposed Guidelines should leave as optional, and not require, originator CASPs to disclose additional personally identifiable information to beneficiary CASPs -** the Proposed Guidelines should not go beyond the Level 1 mandate and should enable CASPs to use their discretion to determine the appropriate information to disclose to beneficiary CASPs when other PII collected is insufficient to clearly identify the originator. This would mean AML objectives together with EU data minimisation and proportionality objectives are met, mitigating privacy and security concerns, and would be consistent with travel rules adopted in other jurisdictions, such as Singapore.
3. **The Proposed Guidelines should permit CASPs to use their own risk-based measures to determine when to collect information regarding SHW counterparties rather than require CASPs to collect such information from their customers in all circumstances. Verification should not be required up to EUR 1,000 -** the Proposed Guidelines should not go beyond the Level 1 provisions and risk-based measures should be adopted in relation to the collection (and verification) of the ownership or control of SHWs. Verification of ownership should not be a mandatory requirement up to EUR 1,000.
4. **The Proposed Guidelines should clarify the suitability of the technical means for verifying ownership of a self-hosted wallet and require a minimum of one technical means (rather than requiring a minimum of**

two) - CASPs should have discretion to manage risks through the verification of SHW address ownership for transactions exceeding 1,000 EUR, and this should be done using a minimum of one rather than two technical means. This is on account of the fact that any one of the proposed means may effectively establish control applying 'adequate' (i.e., risk-based) measures.

1. **The Proposed Guidelines Should Encourage CASPs to Adopt Travel Rule Compliance Solutions that Prioritize Data Privacy and Security, Robust Counterparty Due Diligence Reviews, and Global Coverage.**

Coinbase appreciates that the Proposed Guidelines acknowledge that CASPs may use technological solutions for compliance with the Travel Rule.[2] However, as one of the world's largest global CASPs, we also recognize that not all technological solutions are alike in terms of their ability to overcome the unique challenges of applying the travel rule to cryptoasset transactions while also meeting other, similarly crucial needs—such as ensuring that sensitive customer data remains private and secure. We therefore recommend that the Proposed Guidelines advise CASPs to take a holistic approach when adopting a Travel Rule compliance tool, which would include considering whether the tool appropriately prioritizes data privacy and security, provides robust counterparty due diligence reviews, and offers broad global coverage.

A key hallmark of an effective travel rule tool is the breadth of its coverage—*i.e.*, the extent to which the tool allows a CASP to exchange travel rule information as to a large proportion of its transactions and with a broad spectrum of its counterparties. As described below, we believe that one solution in particular—the industry-led, not-for-profit Travel Rule Universal Solution Technology ("TRUST")—will become a universally adopted tool for international travel rule compliance, much like SWIFT has done for traditional finance.

Although TRUST has taken the leading role in allowing CASPs to meet their travel rule requirements, there remain other travel rule tools—most of which are profit driven—that do not provide comparable security and privacy safeguards, nor do they provide effective governance over the use of their tools to ensure CASPs actually comply with the travel rule. The availability of multiple travel rule tools has led some commentators to mistakenly suggest that building interoperability between those tools could narrow coverage gaps.[3] But the opposite is true: requiring (or otherwise strongly

---

[2] *See* European Banking Authority, *Guidelines on Preventing the Abuse of Funds and Certain Crypto-assets Transfers for Money Laundering and Terrorist Financing Purposes under Regulation (EU) 2023/1113* ¶ 15 (Nov. 24, 2023) (hereinafter the "Proposed Guidelines").

[3] *See* Financial Action Task Force, *Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers*, ¶ 188 (2021),

pressing for) interoperability between travel rule tools would *discourage* CASPs from adopting these tools.

The reason being that, for multiple tools to be interoperable with one another, they must necessarily cater to whichever tool has the *lowest* security and privacy standards. For example, certain tools may store sensitive customer information in centralised databases vulnerable to cyber thieves. Or they fail to conduct robust due diligence reviews of its participating CASPs before sharing sensitive customer data with them. The weaknesses in one tool, by their very nature, are often incompatible with, and could undermine, the protections of other, strong travel rule tools, should they attempt to become interoperable with one another. In other words, a chain of interoperable travel rule tools is only as strong as its weakest link. CASPs around the world recognise this vulnerability, and many are reluctant to adopt an interoperable travel rule tool, no matter how (ostensibly) broad its coverage, if it compromises the privacy and security of customer data, with the myriad legal and reputational risks that poses to CASPs.

Coinbase appreciates that the EBA, through the Proposed Guidelines, is taking an effective approach to Travel Rule compliance by directly collaborating with the crypto industry to solve a complex regulatory problem. And the industry has successfully responded; Coinbase has worked alongside a large group of CASPs over the last few years to pioneer the development of TRUST—a travel rule solution that (1) allows CASPs to accurately identify their counterparties and securely exchange required data, (2) provides a governance structure to adapt to new global requirements, (3) monitors for members' compliance with travel rule requirements, and (4) thoroughly vets the privacy and security standards of all members.[4] While TRUST provides a complete solution to travel rule compliance, other tools may address one part of travel rule compliance (such as the need to send the travel rule information to a CASP counterparty), but lack TRUST's privacy and security standards, potentially jeopardizing sensitive customer information. Coinbase and other leading CASPs have invested significant legal, compliance, engineering, and other resources to build the TRUST solution, which CASPs around the world are already using to exchange information required under the Travel Rule.

TRUST's rapid growth since its launch in 2022 is a testament to the industry's commitment to solving complex compliance challenges. For example, TRUST includes a mechanism for the recipient CASP to *prove* that it is the owner of the receiving crypto address before customer information is sent—to ensure the right information is sent to

---

https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.pdf.

[4] *See* Coinbase, *The Standard for Travel Rule Compliance: Travel Rule Universal Solution Technology*, https://www.coinbase.com/travelrule (last visited Jan. 22, 2024) (describing the TRUST platform and listing CASPs who have joined the TRUST coalition).

the right CASP. Other travel rule tools do not offer this critical feature. Further, TRUST was designed so that no customer personal identifying information is stored on a centralized database but is instead only shared directly between counterparty CASPs via encrypted, peer-to-peer channels, reducing the risk of hacking or improper access—unlike a for-profit vendor tool that merely allows an originating CASP to send an encrypted email to an *unverified* recipient CASP, with no assurances that the recipient CASP will properly open, ingest, and store the sensitive information. Importantly, CASPs who join TRUST must first undergo comprehensive due diligence reviews to help ensure that their security protocols are equipped to prevent unapproved access to sensitive customer data shared by TRUST participants.

As we have noted, unlike travel rule tools provided by for-profit vendors, TRUST is a not-for-profit solution, designed *by* industry *for* industry. The growth and operation of TRUST is overseen by its member CASPs, who convene regularly to discuss and vote on proposals, admit new members, and decide how to enhance the TRUST platform. These and other features have been critical to TRUST's expansion to become the world's leading Travel Rule solution; it today includes over 90 members (including many of the largest CASPs in the world) from 18 countries, including Germany, the United Kingdom, the United States, Singapore, Japan, Hong Kong, and others.

Equally critical was that Coinbase and other CASPs engaged closely and repeatedly with regulators and policymakers around the world while designing and launching TRUST. This approach of collaboration and encouraging industry innovation has proven very effective—as compared to issuing rules without industry input on the actual risk, unintended consequences, and alternatives available. We thank the EBA for seeking industry input to collaboratively understand other risks and develop effective solutions, and we would be delighted to provide the EBA with more details about TRUST.

coinbase

For the reasons discussed above, Coinbase respectfully recommends that the EBA amend the Proposed Guidelines as follows:

Proposed Guidelines	Recommended Amendments
Guideline 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.	**Guideline 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,~~ accurately identifying CASP and ICASP counterparties; b. considering the compatibility with existing industry standards, protocols, and blockchain networks to facilitate integration, including its ability to enable CASPs to exchange travel rule information as to a large proportion of their eligible transactions and with a broad spectrum of their counterparties; and c. assessing data privacy and security, data integration and data reliability.

2. The Proposed Guidelines Should Allow, but not Require, Originator CASPs to Disclose Additional Personally Identifiable Information to Beneficiary CASPs.

Coinbase appreciates that the Proposed Guidelines provide guidance to help originator CASPs identify the originator when the personally identifiable information ("PII") provided to the beneficiary CASP is insufficient to clearly identify the originator. However, the Proposed Guidelines *require* originator CASPs to share sensitive PII—date and place of birth—with beneficiary CASPs in this circumstance,[5] which not only presents privacy and security concerns but also goes beyond what the Level 1 text of the Travel Rule

[5] *See* Proposed Guidelines ¶ 26 (emphasis added).

requires. We therefore recommend that the Proposed Guidelines provide originator CASPs discretion to determine the appropriate information to disclose to beneficiary CASPs when other PII collected is insufficient to clearly identify the originator.

The Travel Rule already requires originator CASPs to provide sensitive PII to beneficiary CASPs. Specifically, Article 14(1) of the Travel Rule requires originator CASPs to "ensure that transfers of cryptoassets are accompanied by the following information on the originator . . . the name of the originator . . . the originator's distributed ledger address . . . the originator's address, including the name of the country, official personal document number and customer identification number, or alternatively, the originator's date and place of birth."

However, the Proposed Guidelines would go a step further, requiring CASPs to disclose even more sensitive PII. Proposed Guideline 26 states that originator CASPs should disclose "*date and place of birth in addition to* the address and official personal document number" when the "name, the account number, address and the official personal document number prevents the unambiguous identification of the . . . originator."[6]

Sharing sensitive PII between CASPs is, of course, necessary under the Travel Rule. But without appropriate protections in place, sharing PII can also present significant privacy and security concerns. For instance, bad actors could exploit CASP information security deficiencies to obtain sensitive PII and link the relevant consumer's identity to a wallet address, revealing all of the consumer's transactions ever made on the blockchain. The "sunrise issue" exacerbates these privacy and security concerns—many countries around the world have not yet implemented, or are still in the early stages of implementing, a travel rule. This results in instances where a CASP in one country (where a travel rule applies) may conduct transfers with foreign counterparties who are not subject to a travel rule and therefore may be less likely to have sufficient information security controls to receive and adequately safeguard sensitive PII.[7]

Accordingly, rather than *require* originator CASPs to disclose sensitive PII beyond what the Level 1 text of the Travel Rule requires, Proposed Guideline 26 should enable originator CASPs to use discretion to determine the appropriate information—date and place of birth or other information—to disclose to beneficiary CASPs when other PII

---

[6] *See* Proposed Guidelines ¶ 26 (emphasis added).
[7] *See* FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* ¶ 196 (Oct. 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf (explaining that a CASP would "need to conduct due diligence on their counterparty [CASP] before they transmit the required information to avoid dealing with illicit actors or sanctioned actors unknowingly," and further to "determine whether a counterparty can reasonably be expected to protect the confidentiality of information shared with it").

collected is insufficient to clearly identify the originator. In addition to mitigating privacy and security concerns, this approach would be consistent with travel rules adopted in other jurisdictions, which provide originator CASPs discretion to disclose the customer's date and place of birth rather than requiring such disclosure.[8]

Considering the comments above, Coinbase respectfully recommends that the EBA amend the Proposed Guidelines as follows:

Proposed Guidelines	Recommended Amendments
Guideline 26: Where the information on the name, the account number, address and the official personal document number prevents the unambiguous identification of the payer or originator, 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.	**Guideline 26:** Where the information on the name, the account number, address and the official personal document number prevents the unambiguous identification of the payer or originator, the payer's PSP or the originator's CASP ~~should~~ may transfer ~~the~~ any additional information it finds necessary for the unambiguous identification of the payer or originator, such as the information on the date and place of birth ~~in addition to the address and official personal document number~~.

3. The Proposed Guidelines Should Permit CASPs to Use Risk-Based Measures to Collect Information Concerning a Counterparty Using a Self-Hosted Wallet.

Coinbase supports the Proposed Guidelines' efforts to clarify how CASPs should collect identifying information regarding counterparties using SHWs. However, the Proposed Guidelines require CASPs to collect information from their own customers to identify SHW counterparties, which may not be feasible in many circumstances because the customers sometimes do not possess this information. Accordingly, we recommend that the Proposed Guidelines permit CASPs to use their own risk-based measures to collect information regarding SHW counterparties rather than require CASPs to collect such information from their customers in all circumstances. Further, verification for SHW transactions should not be mandatory below EUR 1,000.

---

[8] For example, the travel rule in Singapore provides originator CASPs discretion to disclose date and place of birth information to beneficiary CASPs in all circumstances. *See* Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Services Licence (Digital Payment Token Service) ¶ 13.6, https://www.mas.gov.sg/-/media/mas-media-library/regulation/notices/amld/psn02-aml-cft-notice---digital-payment-token-service/notice-psn02-last-revised-on-1-march-2022.pdf.

coinbase

The Travel Rule requires originator CASPs and beneficiary CASPs to collect certain information regarding the counterparty for transfers to or from a SHW.[9] Proposed Guideline 67 requires that CASPs collect this information from their customer: "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*."[10]

However, the collection of this information from the CASP's customer may not be feasible in many circumstances and could result in inaccurate or unreliable information. Some CASP customers may fail to collect the name of a counterparty using a SHW, such as a merchant that accepts payment for its goods or services from a consumer's SHW. Rather than requiring CASPs to collect information from customers that customers do not always have, Proposed Guideline 67 should enable CASPs to take a risk-based approach to identify SHW counterparties.

This approach would align with the EU's AML Directive ("AMLD V"), which requires CASPs to take "mitigating measures" to "identify and assess the risk of money laundering and terrorist financing associated with transfers of cryptoassets directed to or originating from a self-hosted address," including the option to implement "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."[11] Given this flexible, risk-based approach permitted under AMLD V for CASPs to identify SHW counterparties of their customers, Proposed Guideline 67 should similarly permit CASPs to collect information regarding SHW counterparties pursuant to risk-based measures rather than require CASPs to collect such information from their customers in all circumstances.

Further, we recommend revising Proposed Guideline 67 to reflect that verification is required only when the relevant transaction is over 1,000 EUR, as specified in the Level 1 text of the Travel Rule: "In the case of a transfer to or from a self-hosted address, the crypto-asset service provider should collect the information on both the originator and the beneficiary, usually from its client. A crypto-asset service provider should in principle not be required to verify the information on the user of the self-hosted address. Nonetheless, in the case of a transfer of an amount exceeding EUR 1 000 that is sent or received on behalf of a client of a crypto-asset service provider to or from a self-hosted

[9] *See* Travel Rule Article 14(5), 16(2).
[10] *See* Proposed Guidelines ¶ 67 (emphasis added).
[11] *See* Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on Information Accompanying Transfers of Funds and Certain Cypto-assets and Amending Directive (EU) 2015/849 Article 19(a).

address, that crypto-asset service provider should verify whether that self-hosted address is effectively owned or controlled by that client."[12]

Considering the comments above, Coinbase respectfully recommends that the EBA amend the Proposed Guidelines as follows:

Proposed Guidelines	Recommended Amendments
Guideline 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.	**Guideline 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~~ collect such required information pursuant to their risk-based measures. 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.

4. **The Proposed Guidelines Should Clarify the Suitability of the Technical Means for Verifying Ownership of a Self-Hosted Wallet.**

Coinbase appreciates that the Proposed Guidelines specify the technical means that CASPs should use to verify ownership of a SHW for transfers exceeding EUR 1,000. We recommend that Proposed Guideline 69 is revised, so that two or more technical means for verification of ownership is recommended only for cases where it proves necessary, taking a risk-based approach. This would enable a better balance between risk-management, innovation, and compliance burden. Further, the difference between two of the technical means listed is unclear. Coinbase therefore recommends that Proposed Guideline 69 is amended to (1) require the use of at least one of the technical means listed, and (2) remove either of the two technical means that appear identical, or alternatively, clarify any difference between them.

Proposed Guideline 69 specifies technical means that CASPs should use to verify whether a SHW is owned by the customer in the event a transfer to or from a SHW that

[12] *id.* at Recital 39.

exceeds €1,000.[13] Although any one of the technical means listed in Proposed Guideline 69 is sufficient to verify ownership of a SHW, it requires CASPs to use at least two of the technical means listed. For instance, this listed technical means—"attended verification as specified in the 'Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849'"— requires a CASP that uses employees for remote identity verification to establish robust remote identity verification procedures, including developing a detailed interview guide for the employees' use, and therefore this means seems sufficient by itself to verify ownership of the SHW. Requiring the use of a second listed technical means seems to impose an operational burden on CASPs without any material corresponding benefit.

Further, the difference between two of the technical means listed in Proposed Guideline 69 is unclear. Specifically, the first calls for "signing of a specific message in the account and wallet software, which can be done through the key associated with the transfer," while the second entails "requesting the customer to digitally sign a specific message into the account and wallet software with the key corresponding to that address." Both of these technical means, in essence, require a digital signature effected by the customer's key and thus it is unclear how they are different from one another.

We therefore recommend that Proposed Guideline 69 is revised to (1) require the use of at least one (not two) of the technical means listed; and (2) remove one of the two technical means requiring a digital signature effected by the customer's key, or alternatively, clarify any difference between them.

[13] *See* Proposed Guidelines ¶ 69.

coinbase

Specifically, Coinbase respectfully recommends that the EBA amend the Proposed Guidelines as follows:

Proposed Guidelines	Recommended Amendments
Guideline 69: Where the amount of a transfer from or to a self-hosted address exceeds 1 000 EUR, the orig- inator'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: . . . 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.	**Guideline 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~~ one of the following: . . . ~~e. signing of a specific message in the account and wallet software, which can be done through the key associated with the transfer;~~ ~~f.~~ e. requesting the customer to digitally sign a specific message into the account and wallet software with the key corresponding to that address; ~~g.~~ f. 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.

coinbase

***

Coinbase appreciates the opportunity to respond to the EBA's consultations on its guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under the Transfer of Funds (TFR) Regulation (EU) 2023/1113 to develop sound, effective regulation on these and other important issues. We look forward to additional opportunities to collaborate on how best to combat illicit finance.

Sincerely,

Grant Rabenn
Director, Financial Crimes Legal
Coinbase