VASPnet.

23 February 2024

Sent via online form submission via:

https://www.eba.europa.eu/publications-and-media/events/consultation-guidelines-preventing-abuse-funds-and-certain-crypto

To whom it may concern,

We fully support the collaborative efforts made by the European Banking Authority (EBA) to offer guidance to firms required to comply with the so-called 'Travel Rule', through the delivery of the *Guidelines on preventing the abuse of funds and certain crypto-assets transfers for ML/TF (Travel rule Guidelines)*.

We express our gratitude for the opportunity to contribute to the consultation process on the Travel rule Guidelines and remain firmly of the opinion that our collective effort to enhance the regulatory framework for crypto-assets and funds transfers is crucial for the advancement of financial security and compliance.

The guidance provided in the Guidelines, especially regarding the determination of payments made for goods and services, and the handling of incomplete or ambiguous information, is highly appreciated. These efforts significantly contribute to the clarity and enforceability of compliance measures.

Furthermore, participation in the virtual public hearing held by the EBA on January 17, 2024, proved insightful, clarifying the importance of identifying and managing counterparty and intermediary CASP risks as foundational elements for regulatory compliance.

We welcome the opportunity to further elaborate on any of the points included within this response and look forward to continuing to contribute to the implementation stages of the Transfer of Funds Regulation (ToFR).

About VASPnet

VASPnet is the world's assured source of regulatory reference data on virtual asset service providers (VASPs). Our VASPdata platform gives public and private sector entities the information they need to make well-informed, risk-based decisions on the VASPs they do business with. VASPnet is an XReg company, an international public policy and regulatory affairs consultancy specialising in cryptoassets.

General feedback and recommendations

In the Travel Rule guidelines, the central theme on which a firm must apply the guidance is the identification and risk management of counterparty and intermediary Crypto-Asset Service Providers (CASPs).

As such, an obliged entity must, among other undertakings, identify and verify it's counterparty's compliance standards, geographical location, customer profile, adherence to the travel rule, and the solution providers they employ. This evaluation determines if the counterparty fits within the firm's risk appetite.

We believe that this foundational aspect should be prominently addressed in future guidance, emphasizing a risk-based approach to Counterparty CASP Due Diligence.

To complement this stance, if deemed appropriate, we suggest that the EBA take appropriate steps to offer guidance to firms to convey that, in accordance with Regulation (EU) 2016/679 (GDPR), only such data that is required to comply with third country implementations of the travel rule (should it be to a reduced data standard than that specified by the ToFR) be transferred, and not the full data payload as required under ToFR, which has been considered to be of a higher standard than that mandated by the Financial Action Task Force (FATF).

Specific feedback

Section 4, Guidelines 3.1, Paragraph 11.

It should be clarified that adherence to industry data standards can mitigate the risks associated with handling varying data formats and the potential for errors and omissions. The IVMS 101.2023 data standard, developed by the InterVASP Standards Working Group (ISWG) [1], exemplifies a widely recognized framework that ensures consistency in both the structure and content of data payloads. Recognised by the Financial Action Task Force (FATF), this standard may prove highly beneficial for CASPs looking to implement a standardised approach to data transmission. While a common data standard introduces an island of interoperability, there are further considerations on harmonisation, as presented in our response to Section 4, Guidelines 3.1, Paragraph 15.

Section 4, Guidelines 3.1, Paragraph 15.

Interoperability in the context of the Travel Rule involves several dimensions beyond aligning just the technical transmission of required information, which is influenced by a range of non-technical factors. Such inherent heterogeneity in implementation of solutions, legal and regulatory landscape and internal policies may require clarity in both nomenclature and guidance.

Key considerations include:

- Identity: Ensuring that the counterparty is the CASP with which a transfer has been executed or will be executed.
- Transaction Flow: Clarification is needed regarding at what stage the data exchange should occur—whether prior to, or simultaneously with, the execution of a transaction. Both parties should operate to the same transaction flow to facilitate interoperability.
- CASP Due Diligence: The due diligence processes by Travel Rule Solution Providers (TRSPs) can differ significantly, from open networks with broad access to closed networks with strict membership criteria. A global standardisation of due diligence practices is essential for interoperability to work effectively.
- Legal Requirements: Differences in legal requirements across jurisdictions, such as in the EU, may impose additional burdens on TRSPs and affect their business case for supporting additional data sharing protocols.

For a better understanding of interoperability, firms may benefit from additional guidance on functional aspects, specifically:

- Discovery: How to identify a counterparty that may be using a TRSP other than the one to which the firm is registered.
- Due Diligence: The extent to which due diligence has been conducted, its standards, and how to verify such due diligence.
- Payload Structure: Whether the payload is structured in compliance with industry standards (for example, IVMS 101.2023).
- Transmission Protocol: The protocols used for transmission, and considerations with respect to features or limitations owing to their implementation, and whether they are proprietary or open standards.
- Jurisdictional Variances: How regional legal differences may impact the standard of the data payload required.

[1] https://www.intervasp.org

Section 4, Guidelines 3.1, paragraph 15.a

We request that further clarity is offered on Section 3.1, paragraph 15.a, which reads:

> evaluating the protocol's interoperability features to ensure it can seamlessly communicate with other systems, both within and outside CASPs and ICASPS

Specifically, the intention of the clarification '*both within and outside CASPs and ICASPS*'.

Section 4, Guidelines 5.1

When handling incomplete information accompanying transfers, it would be valuable to recognise that variances in compliance requirements across jurisdictions can lead to instances where data, while aligned with the originating CASP's local regulations, may not fully meet the standards outlined in the ToFR. Therefore, allowances should be made for such scenarios to facilitate a more harmonious integration of global travel rule adherence, without penalizing CASPs who act in good faith within their regulatory frameworks.

Section 4, Guidelines 5.3, Paragraphs 34.b and c.

While the current guidelines correctly stipulate that Intermediary CASPs (ICASPs) must ascertain whether the originating or beneficiary CASPs are based in regions subject to restrictive measures or financial sanctions, or in jurisdictions with a high risk of circumvention of restrictive measures, there is no reciprocal expectation outlined for the originating and beneficiary CASPs to evaluate such risks linked to the ICASPs in the transfer chain. It is crucial to stress the importance of understanding not only the counterparty risk but also the data handling practices in alignment with Regulation (EU) 2016/679 (GDPR).

Compliance with GDPR is not merely a legal requirement but also an essential aspect of maintaining trust and integrity in the transfer of funds. Thus, the guidelines would benefit from addressing the need for CASPs to implement robust systems and controls for the handling of personal data to ensure GDPR compliance across all parties involved in the transfer chain.

We note that in the identification of risk factors as presented in Paragraph 34 does not include seeking clarity on the CASP or ICASP's regulatory status. While it is evident within Paragraph 34 that the obliged entity should ascertain geographic risks, which includes whether the country is subject to restrictive measures, or present in a country in which the obligation to obtain and hold data does not exist, we note ToFR, Paragraph 60, which states:

> Based on the information gathered, the correspondent crypto-asset service providers should implement appropriate risk mitigating measures, which should take into account in particular the potential higher risk of money laundering and terrorist financing posed by unregistered and unlicensed entities.

As such, we propose inclusion of the following text as a new limb of Paragraph 34:

> transfers from or to accounts, addresses or wallets known to be linked with CASPs that are operating without authorisation to do so in their jurisdiction of domicile, service or operations;

Section 4, Guidelines 6.1, *Paragraphs 48 through to 59*

When it comes to returning a transfer, there are notable technical and operational hurdles that need to be overcome. Technical restrictions on certain types of crypto-assets prevent them being returned to the original sending address, which could result in an increased number of orphaned transactions as adherence to the travel rule becomes more widespread.

To address this, we suggest that transfer information include a designated 'Ordering CASP Return Address'. This would facilitate the Beneficiary CASP in promptly returning transfers that cannot be accepted, not due to Financial Crimes or Sanctions issues, but rather because of incomplete Required Information.

Furthermore, the nature of blockchain technology does not support the rejection of transfers post-execution. We propose that further consideration is given to an agreement of a transfer flow that will ensure that consideration on the acceptance of said transaction occurs in advance of execution of the transfer, thus preventing the need for post-transaction reversals.

Section 4, Guidelines 8.2.1, Paragraph 65.

Determining whether a transfer originates from, or is destined for, a self-hosted wallet is challenging due to the current technical limitations in accurately or precisely identifying wallet ownership[2]. This uncertainty raises the question of the extent to which CASPs can depend on the information provided by the transfer originator.

Guidance may be of value as to what data from customers could be captured relating to on the presence, and identity, of a counterparty – including trading names, brand names, legal entity names, or Legal Entity Identifiers (LEIs). This would facilitate the Originating CASP in determining the most effective way to share the required data with their counterparty.

Furthermore, the quality of data, especially in the identification of counterparties, poses a significant obstacle in due diligence processes and regulatory reporting for financial institutions. Addressing risks associated with data management by leveraging broadly adopted third-party reference datasets[3] could be instrumental. This approach would allow CASPs to conduct additional testing and verification before disseminating Personally Identifiable Information (PII).

[2] FATF Updated Guidance VA and VASPs, paragraph 156.d. footnote 39: 'To date, FATF is not aware of any technically proven means of identifying the person that manages or owns an unhosted wallet, precisely and accurately in all circumstances.'

[3] For example, VASPnet (https://www.vaspnet.com)