VASPnet.

28 July 2026

Submitted via email to: FATF.Publicconsultation@fatf-gafi.org

To whom it may concern,

Re. The Financial Action Task Force (FATF) Public Consultation – Guidance on Implementation of FATF Recommendation 16

We fully support the collaborative efforts made by the Financial Action Task Force (FATF) to invite stakeholder views and comments on the draft Guidance. We appreciate that the detailed Guidance and practical examples will assist public and private sector stakeholders to effectively implement the requirements as set out in R.16. From the perspective of participants in the virtual asset service provider (VASP) industry, such guidance has proven crucial in global harmonised implementation of this Recommendation.

We express our gratitude for the opportunity to contribute to the consultation process and remain firmly of the opinion that our collective effort to enhance the regulatory framework for virtual assets and payment transparency is crucial for the advancement of financial security and compliance.

Given VASPnet's role as a regulatory reference data provider, our response focuses on clarity of information exchange, a risk-based approach to counterparty due diligence and consistency in party identification. We welcome the opportunity to elaborate further on any of the points included within this response and look forward to continuing our positive, constructive dialogue directly and by way of the Virtual Asset Contact Group (VACG).

Yours faithfully,

Neil Samtani, **CEO, VASPnet**

About VASPnet

VASPnet is the world's assured source of regulatory data on virtual asset service providers (VASPs). Our VASPdata and VASPindex products give 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 a division of CRB Monitor, a global data provider focused on newly regulated markets. To find out more, visit vaspnet.com and follow us on LinkedIn.

Contact us at info@vaspnet.com

General feedback and recommendations

We welcome the FATF's work to provide a more standardised and consistent framework for implementing Recommendation 16. It remains our belief that greater consistency in the interpretation and implementation of payment-transparency requirements will reduce regulatory fragmentation and enable financial institutions (Fis) to apply more effective and proportionate controls. We particularly support the emphasis on structured data, clearer allocation of responsibilities across the payment chain and the principle that obligations should follow the activity performed rather than the legal form or the name of the entity.

We believe it is important that the Guidance remains payment-method-neutral and technology-neutral. At the same time, we should remain conscious of the specific characteristics of virtual asset transfers that may introduce novel risks or operational and implementation challenges. Virtual asset transfers can be instantaneous and irreversible and may operate through payment chains that are semi-intermediated rather than through established bilateral or correspondent relationships. An ordering VASP may know its customer and the destination wallet address but may not have the means to immediately know whether that address is controlled by another VASP, a self-hosted wallet or another type of intermediary.

The Guidance notes that VASPs are subject to R.16 through the Interpretive Note to Recommendation 15 (7.b), that virtual asset and hybrid payment chains may form part of a single payment chain, and that the virtual asset sector has developed modern Travel Rule and pre-validation solutions. We recommend that these considerations be complemented with guidance explaining how the underlying objectives of R.16 are to be achieved where the identity of the counterparty institution is not evident from the payment instrument or address itself.

The ability to identify the financial institution or VASP at the other end of a payment is fundamental to effective implementation. This is particularly important in partially disintermediated payment models. Specifically, where a payment chain may or may not be bookended by a VASP or other financial institution.

We welcome FATF's acknowledgement that R.16 should not negatively affect legitimate access to financial services, and measures should remain proportionate and risk-based. Clarifying the distinction in risks between correspondent relationships (as present in Recommendation 13) and those evident between payment counterparties may help to meet the objective of faster, less costly, safer, more transparent and more inclusive cross-border payments through clarity in guidance on counterparty due diligence. An example of such an implementation is in Article 19b of the EU's Transfer of Funds Regulation (2023/1113)[1], whereby a CASP is expected to undertake due diligence on a 'correspondent' (transfer or payment institutional counterparty) should they not be 'established in the Union'.

We support the attention given to virtual account numbers and vIBANs. As the Guidance recognises, an ordering or intermediary institution may be unable to distinguish a virtual account number from a conventional account number. The resulting lack of visibility can obscure both the institution that services the underlying account and the jurisdiction in which it is located, preventing institutions from understanding the true nature of the payment.

The Guidance correctly recommends that countries establish a clear domestic legal basis for collecting, processing, transmitting and storing R.16 information, conduct gap analyses between AML/CFT/CPF and privacy frameworks, and provide a lawful basis for cross-border transfers. It also recognises that destination-country requirements can create uncertainty and that competent authorities may need to resolve conflicts through domestic and cross-border coordination.

Financial institutions and VASPs should not be placed in a position in which compliance with R.16 creates an apparent breach of national privacy law, as may arise in jurisdictions with restrictive consent, overseas-transfer or localisation requirements.

All too often, the Travel Rule is reduced to a requirement to transmit specified fields. The underlying purpose of ensuring that meaningful information concerning the originator, beneficiary and relevant institutions is available to detect and investigate money laundering, terrorist financing, proliferation financing, fraud and other illicit activity must not be ignored.

With that objective in mind, and given that full implementation of the proposed language in the Guidance is not expected until the end of 2030, the Guidance must be capable of accommodating payment methods, settlement arrangements and forms of intermediation (and disintermediation) that may not yet exist.

In rapidly evolving sectors, such as virtual assets, illustrative examples should be anchored to durable principles, including the identification of parties and institutions involved in a payment, preservation of information across the payment chain, reliable attribution, availability of information to relevant institutions and authorities, and the ability to apply effective risk-based controls.

---

[1] Article 19b of Directive (EU) 2015/849, inserted by Article 38(4) of the Transfer of Funds Regulation (EU) 2023/1113, https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng

#	Question	Response summary
1	Are the scope of R.16 and the terminology used clear enough to implement R.16?	Request for further clarity on applicability to technical and ancillary service providers, acknowledgement of technical constraints to VASPs, and alignment with industry standard IVMS 101.
2	Are the principles of payment chain definition and their application clear? Is there any additional guidance that would support PMIs in enabling Fis compliance with the revised R.16?	Proposed clarification on batch transfers, nested VASPs and data veracity.
4	Is the guidance clear on: Information requirements regarding cross-border payments or value transfers? Origin of funds, including when the origin of funds requirements apply and what information needs to be shared when it does?	Comments on the identification of VASPs in payment chains leading to fiat-virtual asset exchange, and in support of the LEI.
11	Does Chapter 8 provide sufficient clarity on how R.16 applies to different payment methods?	In support of technology neutrality, while future-proofing the language as novel payment methods appear.

Specific Responses

1) Are the scope of R.16 and the terminology used clear enough to implement R.16?

The scope and terminology are generally clear. We support the functional approach under which obligations are determined by the activities performed rather than the legal form or description of the relevant entity. However, further clarification would assist implementation in relation to technical service providers, virtual asset transfers, counterparty institutions and the interaction between Recommendations 13, 15 and 16.

Technical and ancillary service providers

Paragraphs 35 and 36 distinguish obliged entities from persons that provide only messaging, technical support or payment infrastructure. We support the exclusion of providers whose role is genuinely limited to the provision of technology or infrastructure. The Guidance should, however, clarify that this exclusion does not apply where a provider also performs activities falling within the definition of a financial institution or VASP. An entity should not fall outside the FATF Standards merely because it describes itself as an infrastructure, software or ancillary service provider where, in substance, it controls assets, executes or facilitates transfers, or conducts another covered activity as a business on behalf of another person.

We propose the final Guidance should therefore focus on the function performed and the degree of control exercised, rather than on the terminology used to describe the provider.

Virtual asset-specific technical constraints

Paragraph 37 appropriately recognises that technical constraints may arise. This recognition should be developed further in relation to virtual asset transfers.

Unlike a conventional payment account, a newly supplied wallet address may not immediately reveal whether it is controlled by another VASP, a self-hosted wallet or another participant. FATF's earlier guidance acknowledges that there is no technically proven method of identifying the VASP managing a beneficiary wallet exhaustively and accurately from the virtual asset address alone[2], although there is an increased likelihood that an address may be attributed to a VASP subsequent to the transfer being executed.

The same guidance also states that Travel Rule information should be submitted before or concurrently with the virtual asset transfer, and that post-facto

[2] FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (October 2021), paragraphs 185, 187 and 197(a), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

submission should not ordinarily be permitted. Accordingly, the final Guidance should confirm that any limited accommodation should apply only to retrospective counterparty attribution, rather than to the retrospective collection and transmission of the required originator and beneficiary information.

Interplay with Recommendation 13

An ordering institution may need to identify and assess a counterparty institution before conducting a payment or value transfer. This is particularly important in the virtual asset sector, where the ordering VASP must determine whether the destination is controlled by another VASP and whether that VASP is an appropriate institution with which to transact and share customer information.

However, identifying and assessing a payment or transfer counterparty should not automatically be treated as equivalent to establishing a correspondent banking relationship. FATF's existing virtual asset guidance recognises that a counterparty VASP relationship may not constitute correspondent banking, although aspects of Recommendation 13 may provide useful reference points for conducting counterparty due diligence.

We believe that the Guidance should clarify the need for ordering institutions to have access to sufficient information to identify and assess the counterparty institution where one is involved. It would be valuable to distinguish between:

- identifying and assessing a counterparty institution for the purpose of an individual payment or stream of payments; and
- conducting more extensive due diligence ordinarily associated with a correspondent banking relationship as specified in R.13.

Furthermore, paragraph 46 appropriately clarifies that Recommendation 16 does not prescribe a particular modality for screening payment information against sanctions lists. The Guidance should nevertheless acknowledge that sanctions risk may arise not only from the originator or beneficiary but also from the financial institution or VASP involved at the other end of the transfer.

Paragraphs 52 and 55 correctly emphasise the need to avoid misclassifying lower risks as higher risk and to preserve proportionality in implementing Recommendation 16. In practice, many VASPs apply full correspondent-style due diligence to every payment counterparty, serving as an example of potentially disproportionate implementation, and which has led to increased costs, delayed transfers and ultimately the de-risking of smaller providers or jurisdictions, even where the underlying risks could be addressed through more targeted controls.

Clearer guidance on this distinction would support effective, risk-based counterparty due diligence without importing the full requirements of Recommendation 13 into every payment-counterparty interaction. It would also advance the objective of making cross-border payments safer, more transparent, less costly and more inclusive while preserving effective AML/CFT/CPF controls.

Alignment with IVMS 101

Paragraphs 49 and 50 recognise the importance of global messaging standards and cooperation with PMIs, SWIFT and CPMI. We support this approach and recommend that the Guidance also recognise the progress already made within the virtual asset sector through IVMS 101.

IVMS 101 is an ISO 20022 compliant standard, and recognised by SWIFT as an innovative model to cater for nascent and rapidly evolving segments of financial services. In the VA space, the standard has been widely adopted as a common data model for exchanging required originator and beneficiary information[3].

Commented [LM1]: I can't find the source of this statement by SWIFT… should we remove it?

The Guidance need not prescribe IVMS 101 as the sole technical standard. Rather, the standard could be presented as an example of one that can coexist with other interoperable messaging frameworks, including ISO 20022. This would remain consistent with FATF's technology-neutral approach.

2) Are the principles of payment chain definition and their application clear? Is there any additional guidance that would support PMIs in enabling FIs compliance with the revised R.16?

We feel the principles are generally clear, particularly the focus on the functions performed by each institution and the requirement to preserve information throughout the payment chain. However, additional virtual asset examples would support consistent implementation.

Batch transfers

For clarity, the Guidance could specify the applicability of batch transfer provisions to virtual asset transfers.

In **paragraph 69** a batch transfer is defined. However, a VASP may execute multiple transfers from a single originator to multiple beneficiaries through a bundled instruction or a single atomic (simultaneous and indivisible) blockchain transaction without a 'file'. While **paragraph 70** offers flexibility in implementation, technical aggregation should not remove the obligation to maintain the required information for each underlying transfer. The flexibility available for batch transfers should apply where each beneficiary and transfer remains individually identifiable and traceable.

---

[3] InterVASP, InterVASP Messaging Standard 101 (IVMS 101), https://www.intervasp.org

Nested VASPs

The Guidance should clarify the treatment of nested VASP arrangements. A nested VASP remains an obliged entity and should not transfer its R.15 or R.16 responsibilities to the VASP providing it with account, wallet or infrastructure access.

Where a host VASP receives and transmits virtual assets on behalf of a nested VASP, without being the ultimate originator or beneficiary, it should ordinarily be treated as an intermediary VASP. It should therefore preserve the required information, identify transfers with missing information and apply appropriate risk-based follow-up measures. The nested VASP should remain the ordering or beneficiary VASP according to the function it performs in the underlying customer transfer. This would reflect the functional definition already applied to intermediary institutions.

Furthermore, Nested VASP relationships may more appropriately fit the definition of Correspondent relationships, and as such, guidance reflecting an interplay with Recommendation 13 may prove helpful.

Completeness and accuracy of information received

The Guidance should also address the veracity of information received from another institution. A beneficiary or intermediary institution should not necessarily assume that information is reliable solely because it has been supplied by a counterparty, and with any such doubts to the veracity of received data, there may be uncertainties to the need to 'take freezing action and prohibiting transactions with designated persons and entities'.[4]

This is particularly relevant where the counterparty is unregulated, operates without required authorisation or is subject to weak supervision. Institutions should be permitted to consider the counterparty's regulatory status, jurisdiction, supervisory framework and history of providing complete and reliable information when applying their risk-based policies.

This should not require transaction-by-transaction re-verification of all originator information. Rather, concerns regarding the counterparty or the reliability of its data should inform decisions on whether to execute, suspend or reject a transfer and whether further information should be requested.

---

[4] FATF, The FATF Recommendations, Interpretive Note to Recommendation 15 (New Technologies), paragraph 7(b), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/fatf-recommendations-2012.pdf

Payment market infrastructure interoperability

We support the proposed emphasis on structured data, consistent identifiers and mapping between payment infrastructures as presented in **section 4.6.**

PMIs should be encouraged to support mapping between standards such as ISO 20022 and established virtual asset messaging standards, including IVMS 101. This would support interoperability while remaining technology-neutral. FATF need not prescribe a single standard, but should encourage interoperable formats that preserve the meaning, structure and integrity of required information across fiat, virtual asset and hybrid payment chains.

Overall, the payment-chain principles were found to be sufficiently clear, and examples covering batch virtual asset transfers, nested VASPs and interoperability would materially improve their practical application.

4) Is the guidance clear on:

- Information requirements regarding cross-border payments or value transfers?
- origin of funds, including when the origin of funds requirements apply and what information needs to be shared when it does?

The draft Guidance is generally clear, but several aspects of virtual asset transfers and hybrid fiat–virtual asset payment chains would benefit from further clarification.

Identification of the VASP in 'on- and off-ramp' transactions

Language in the Guidance should clarify how parties are ideally represented in hybrid payment chains. Where a fiat payment is made to fund an account or wallet at a VASP, the VASP receiving the fiat funds should ordinarily appear as the beneficiary or creditor in the payment message. Where the funds are received for a particular VASP customer, that customer may be identified as the ultimate creditor. We believe that the table 'Thresholds' found in section 5.3 would benefit from a further point of clarity confirming

'where funds are deposited to a financial institution or VASP other than the beneficiary institution or VASP, the name of the financial institution or VASP to which the funds are deposited should be included'.

This is consistent with **Box 7, Case Study 2** under which the CASP appears as the beneficiary and its customer as the ultimate creditor. It would avoid payment messages incorrectly suggesting that the account-servicing institution holds an account directly for the underlying VASP customer. Furthermore, the **principle 'A new instruction begins a new payment or value chain'**, example (1) would benefit from explaining whether MVTS G (beneficiary institution) would be the beneficiary in the payment, or whether it would be Customer Y, and how such data should be conveyed in a payment message.

Thresholds and virtual asset transfers

The Guidance should state more prominently that **all-VA-to-VA transfers should be treated as cross-border**. A cross-reference should therefore be added to Section 5.4 to make clear that the simplified domestic-transfer regime does not apply to VA-to-VA transfers.

Legal Entity Identifiers

We support the encouragement given to the use of LEIs. They provide globally interoperable and publicly accessible reference information that can improve the identification of participating institutions. We are encouraged by the growing adoption of LEIs globally.

11) Does Chapter 8 provide sufficient clarity on how R.16 applies to different payment methods?

Chapter 8 is highly valuable and generally provides sufficient clarity. In particular, we support its functional approach, whereby obligations should depend on how a payment is executed and the role performed by each participant, rather than the label applied to the product or technology.

Technology neutrality and novel payment methods

The final Guidance should emphasise that the examples in Chapter 8 are illustrative rather than exhaustive. New payment methods, proxy identifiers and forms of intermediation (and disintermediation) will continue to emerge before and after implementation in 2030. The enduring test should be whether an entity receives or acts on a payment instruction, holds or transfers value, or merely provides technical support.

Identification of the true parties

Payment messages should distinguish the institutions facilitating the transfer from the ultimate originator and beneficiary. A wallet provider should not be recorded as the debtor or creditor merely because its infrastructure is used, unless it is itself the relevant party to the payment.

Where a payment is made to fund a customer account at a VASP or CASP, the CASP should ordinarily appear as the beneficiary or creditor, with the relevant customer identified as the ultimate creditor. The existing CASP and vIBAN example in **Section 5.5** should therefore be cross-referenced in **Chapter 8**.