Febelfin position regarding the FATF consultation on the Guidance for Recommendation 16

1) Are the scope of R.16 and the terminology used clear enough to implement R.16? (Chapter 3)

We consider that Chapter 3 provides a generally clear framework regarding the scope of Recommendation 16 and the key concepts underpinning it. Nevertheless, further clarification would support consistent implementation across jurisdictions, payment-chain participants, and business models.

Scope

FATF could more clearly distinguish between obligations that are directly within the control of financial institutions and outcomes that depend on payment infrastructures, messaging standards, industry-wide mechanisms, or data availability. Such clarification would help reduce divergent supervisory interpretations and promote a proportionate and operationally realistic implementation of the standard.

While we welcome the inclusion of fraud prevention among the objectives of R.16, fraud and AML/CFT requirements are often subject to different legal, governance, and data protection frameworks. Additional guidance, supported by practical examples, would help clarify how these objectives interact in practice. Similarly, the concept of “misdirected payments” would benefit from greater precision, as such payments may result from operational issues or customer error and should not automatically be treated as fraudulent.

We also welcome the clarification regarding the interaction between Recommendations 16 and 10. However, references to information accuracy and verification could still be interpreted as extending customer due diligence requirements. FATF could therefore clarify that R.16 is intended to support the transmission of accurate payment information and does not create additional CDD obligations. Further distinction between accuracy checks, alignment processes, and CDD measures would support consistent implementation.

Similarly, we welcome the clarification introduced through footnote 49 to INR.16 regarding targeted financial sanctions obligations. In particular, the Guidance confirms that Recommendation 16 does not prescribe whether or how payment information should be screened against sanctions lists and recognises that different mechanisms may be used to ensure compliance with applicable sanctions requirements. This clarification is important to reduce the risk of divergent supervisory interpretations and unnecessary operational friction. FATF could further emphasise that Recommendation 16 should not be interpreted as requiring any specific transaction-filtering methodology where a sufficiently robust sanctions-screening framework is already in place and achieves equivalent compliance outcomes. Further guidance on this point would support a more consistent and proportionate implementation across jurisdictions.

Terminology and interpretative clarifications

Overall, the terminology used in the draft Guidance is sufficiently clear. However, certain interpretative elements appear to go beyond the wording of Recommendation 16 by introducing additional operational expectations or greater flexibility than expressly contemplated by the standard, particularly regarding address requirements and the use of alternative location identifiers (see Question 4.2). Any supplementary guidance should remain closely aligned with the Recommendation and preserve a risk-based, operationally feasible approach.

Further clarification would also be helpful regarding VIBAN arrangements, cross-border cash withdrawals, and the scope of the concept of “payment or value transfer.” Additional examples covering account funding, securities-related transfers, wallet funding, and similar arrangements would enhance legal certainty and consistency of interpretation.

Finally, while we welcome the guidance on LEIs, BICs, and other legal-person identifiers, FATF could further clarify what is meant by “reasonably ascertaining” whether such an identifier exists. It would be useful to confirm that institutions may rely on existing onboarding, CDD/KYC, and customer information processes, without being expected to conduct separate searches or verification activities.

Implementation timeline

Finally, we are concerned that the expectation of full implementation by the end of 2030 may not be realistic for all requirements. Certain measures, particularly those relating to alignment checks, depend on significant legal, technical, and infrastructure developments, including changes to payment market infrastructures (PMIs), messaging standards, and regulatory frameworks, many of which remain under development in several jurisdictions.

As a result, institutions will need to prioritise implementation efforts and, where appropriate, rely on transitional arrangements. We therefore encourage FATF to recognise these dependencies and maintain a degree of flexibility in implementation timelines, particularly where successful implementation is contingent on broader regulatory, industry-wide, or infrastructure-related developments beyond the control of individual financial institutions.

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? (Chapter 4).

We generally consider the payment-chain principles set out in the Guidance to be clear and appropriate. In particular, we support the approach whereby obligations are allocated to the participant that receives, controls, or has access to the relevant information. Nevertheless, further clarification would be beneficial in situations where certain data elements are not available to all participants in the payment chain. Additional guidance in this area would help ensure that responsibilities remain proportionate and aligned with the role, capabilities, and information access of each participant.

In addition, we encourage FATF to recognise more explicitly that compliance with certain aspects of Recommendation 16 is dependent on the evolution of payment market infrastructures (PMIs), messaging standards, scheme rules, and industry-wide data models. Acknowledging these dependencies would help support a realistic and consistent implementation of the standard. Further guidance on the application of R.16 to debit-payment and pull-payment arrangements would also be valuable in promoting a common understanding across different payment models.

Finally, FATF could clarify that Recommendation 16 does not impose an end-to-end responsibility on individual financial institutions where the transmission of information is constrained by PMIs, messaging standards, or other infrastructure limitations. Institutions should be expected to transmit all information within their possession and technical capabilities, but should not be held accountable for information that cannot be transmitted due to limitations beyond their control. Such clarification would provide greater legal certainty and support a proportionate allocation of responsibilities across the payment chain.

3) In the development of the Guidance, emerging practices could be considered where some PMIs offer data storage services that allow participating financial institutions (FIs) to retain required originator and beneficiary information at the PMI. In such models, the PMI holds the required information, and the payment message would only carry a reference to this stored payment data (i.e., token). How could such emerging practices allow FIs to meet their AML/CFT/CPF requirements in particular with regards to accompanying required R.16 information, TFS screening, transaction monitoring, alignment checks, and suspicious transaction reporting? (Chapter 4).

We recognise that PMI data-storage and token-reference models may support the objectives of Recommendation 16 by enabling originator and beneficiary information to be stored centrally and accessed through a reference mechanism, rather than being transmitted in full with each payment message. Such models have the potential to improve efficiency, interoperability, and data consistency across payment chains, provided that participating financial institutions maintain reliable and timely access to the underlying information.

In our view, the key consideration is not the use of tokenisation itself, but whether financial institutions remain able to effectively fulfil their AML/CFT/CPF obligations. Institutions should therefore be able to access the required information without undue delay for the purposes of transaction monitoring, targeted financial sanctions screening, alignment checks, suspicious transaction reporting, investigations, and responses to supervisory, audit, or competent-authority requests. The use of token-reference models should not diminish institutions' ability to comply with, or demonstrate compliance with, their regulatory obligations.

To support the adoption of such models, FATF could provide additional guidance on the conditions under which financial institutions may rely on data held by a PMI. In particular, a clear governance framework would be valuable to clarify the respective roles and responsibilities of PMIs and participating institutions, including with regard to data quality, accessibility, resilience, auditability, security, and data protection. Further clarification on the allocation of responsibilities for AML/CFT controls, targeted financial sanctions compliance, and the retention and retrieval of payment information would also support consistent implementation.

Finally, the Guidance could acknowledge that the effectiveness of these models will depend on the development of common industry standards covering data formats, reference mechanisms, access protocols, and data-management practices. Such standards are essential to ensuring transparency, interoperability, and a consistent implementation of Recommendation 16 across the payment ecosystem.

4) Is the guidance clear on information requirements regarding cross-border payments or value transfers; and origin of funds, including when the origin of funds requirements apply and what information needs to be shared when it does? (Chapter 5).

Overall, Chapter 5 provides a generally clear framework regarding the information that should accompany cross-border payments and value transfers, including the circumstances in which origin-of-funds information should be transmitted. However, several aspects would benefit from further clarification to support consistent implementation and ensure close alignment with Recommendation 16 and its Interpretive Note.

First, the draft Guidance could be interpreted as limiting the flexibility intentionally provided under Recommendation 16 regarding the use of *de minimis* thresholds. While the Standard leaves it to jurisdictions to determine whether and how such thresholds should be applied, paragraphs 176 and 177 may be read as encouraging their adoption. We therefore encourage FATF to preserve this flexibility, allowing jurisdictions to calibrate their approach based on AML/CFT/CPF risks, sanctions considerations, and financial inclusion objectives. In this context, it is also important to recognise that reducing payment-transparency requirements below certain thresholds may impair sanctions screening, transaction monitoring, fraud detection, and alignment checks, as targeted financial sanctions apply irrespective of transaction value.

Second, while we welcome the use of alternative data and fallback options to support financial inclusion, the Guidance should emphasise that such information must remain sufficiently structured, standardised, and interoperable to support payment-transparency objectives. In particular, replacing address information with identifiers that cannot be readily used for screening or monitoring purposes, such as customer reference numbers, may reduce the effectiveness of financial crime controls. Likewise, alternatives to town or village information should provide a sufficiently precise indication of geographic location. While flexibility is appropriate where structured address information is unavailable, overly broad or non-specific location identifiers could undermine sanctions screening, geographic risk assessments, and fraud controls.

We also welcome the clarifications regarding LEIs, BICs, and other legal-person identifiers. However, paragraph 151 could be interpreted as creating an expectation that institutions proactively search for or obtain an LEI where one may exist. To avoid extending existing obligations under Recommendation 16, FATF could clarify that institutions are expected to transmit LEIs that have already been provided by, or obtained from, customers through existing onboarding and CDD processes, rather than being required to source them specifically for payment purposes. More broadly, LEI accuracy and maintenance should remain within established CDD frameworks. The Guidance could also clarify that LEIs are a useful complementary identifier but should not substitute transaction-relevant geographic information, as they do not necessarily reflect the location relevant to a specific transaction.

Finally, we support FATF's objective of ensuring that sufficient information accompanies a payment throughout the payment chain and welcome the alignment with Regulation (EU) 2023/1113 regarding the transmission of the full names of debtors and creditors. To avoid ambiguity, the Guidance could explicitly confirm that initials, abbreviations, or truncated names should not be treated as equivalent to full names where complete information is available. This is particularly important because downstream institutions generally rely on the payment message itself, rather than underlying CDD documentation, to perform sanctions screening, transaction monitoring, and other payment-transparency controls. Additional practical guidance on the application of origin-of-funds requirements across different payment models, funding arrangements, and multi-party payment chains, supported by illustrative examples, would further promote consistent implementation across jurisdictions and payment ecosystems.

5) For cross-border payments or value transfers above de minimis threshold, R.16 requires ordering financial institutions to verify originator's information for accuracy. How feasible is it to verify the originator's address using reliable and independent sources? By what means do you verify the originator's address for accuracy? (Chapter 5)

We welcome the distinction drawn in the Guidance between the verification requirements under Recommendation 16 and customer due diligence obligations under Recommendation 10. In our view, the verification of originator information for R.16 purposes should not be interpreted as creating additional verification requirements beyond those already performed through onboarding, CDD, and ongoing customer information maintenance processes.

In practice, the ability to verify the originator's address is closely linked to the financial institution's relationship with the customer. For the originating institution, address information is typically obtained and verified through established CDD processes and maintained through ongoing customer-information review procedures. The accuracy of the address can therefore be assessed using the same documentation, information sources, and controls that support the institution's broader customer due diligence framework.

The situation is different for beneficiary institutions, which generally do not have access to the underlying customer information relating to the originator. In the absence of a direct customer relationship, independent verification of the originator's address is not realistically feasible on a transaction-by-transaction basis. FATF could therefore usefully clarify that, unless specific risk indicators or inconsistencies are identified, beneficiary institutions may rely on the information transmitted through the payment chain and should not be expected to perform separate verification of originator address information.

More generally, we support a principles-based and risk-based approach, recognising that the means used to verify address information may vary depending on the customer type, product, business model, distribution channel, and risk profile. Where standardised address information or documentary evidence is not readily available, proportionate alternative approaches should remain possible, provided that the information obtained remains sufficiently reliable to support the objectives of payment transparency and AML/CFT/CPF compliance.

6) Does the Guidance provide sufficient examples to support implementation in lower-capacity contexts? (Chapter 5).

Yes. The Guidance adopts a pragmatic approach by allowing alternative verification methods where standard address information is unavailable. This flexibility is important to support financial inclusion and operational feasibility while preserving the overall objectives of payment transparency.

7) Regarding virtual account numbers, the Guidance presents a non-exhaustive list of measures to ensure compliance with the requirement set out in INR.16, paragraph 7, particularly that FIs should ensure that account numbers should not be used to disguise the identification of the country where the FI that services the account resides. To what extent are these measures sufficiently clear and actionable? What other measures have you identified to meet this requirement? (Chapter 5).

We consider that the measures set out in the Guidance are generally clear and operationally workable and provide a useful basis for achieving the transparency objectives of Recommendation 16 in the context of virtual account number arrangements.

Nevertheless, further clarification would be beneficial regarding the allocation of responsibilities. Consistent with Recommendation 16 and paragraph 162 of the draft Guidance, FATF could expressly clarify that the responsibility for ensuring that account numbers are not used to disguise the identification of the country in which the servicing financial institution resides lies with the financial institution that owns the underlying master account and services the virtual account or virtual IBAN. In practice, other participants in the payment chain often have limited, or no, visibility over the existence of a virtual account structure, the underlying master account, or the way in which the virtual account number has been configured. Imposing such responsibility on those institutions would therefore be operationally unrealistic and could create expectations that cannot be effectively implemented.

More generally, the Guidance could further emphasise that virtual account arrangements should not obscure the cross-border nature of an underlying account relationship or create the appearance of a domestic transaction where the servicing arrangement is in fact cross-border. While legitimate treasury, liquidity-management, reconciliation, and operational arrangements should continue to be supported, payment-chain participants and competent authorities should remain able to identify the servicing financial institution and the relevant jurisdiction in a reliable and consistent manner.

Finally, we note that a number of jurisdictions are already developing specific mechanisms to enhance transparency in virtual account arrangements. For example, the European Union has opted for a centralised repository approach to facilitate the identification of virtual IBANs. FATF may therefore wish to recognise that the objectives of Recommendation 16 can be achieved through different regulatory and technical solutions, including centralised registries, repository-based mechanisms, prefixes, or other transparency-enhancing tools. The Guidance should remain sufficiently flexible to accommodate existing and future regional initiatives and avoid favouring a single implementation model where alternative approaches can deliver an equivalent level of transparency.

8) Are the explanations of the roles of key participants, including card issuers, acquirers, payment facilitators, sponsored issuers, and card networks appropriate in light of the technical nature of card payments? (Chapter 6).

While the explanations provided in Chapter 6 are generally useful, further clarification would be welcome regarding the role of certain actors in the card-payment ecosystem. In particular, the concepts of payment facilitators and payment aggregators, which are referred to several times in the Guidance, could usefully be defined to promote a common understanding of their role and responsibilities under Recommendation 16. Additional guidance on sponsored issuers would also be beneficial, as their identification may be challenging in practice due to differences in the information available across card networks, non-harmonised naming conventions, and evolving BIN allocations. Acknowledging these operational constraints would help support the effective implementation of sanctions screening and other financial crime controls.

9) In distinguishing between card transactions for the purchase of goods or services and other card-funded payments (e.g., a person-to-person transfer, including card top-ups), are the conditions set out in paragraph 190 clear to identify person-to-person transfers? (Chapter 6).

Further guidance would be welcome on the scope of the exemption for purchases of goods and services, including additional examples illustrating how it applies in practice. In particular, clarification would be beneficial for scenarios such as charitable donations and quasi-cash transactions, including the purchase of casino chips, crypto-assets, or deposits to gambling platforms, as well as through a clearer definition of the concepts of “goods” and “services”.

10) Chapter 7 (Section 7.3 Information requirements for cash withdrawals) explains what types of transactions fall within the scope of ‘cash withdrawals’. It covers all types of transactions in which a cardholder accesses cash using a payment card, including cash withdrawals via ATM and cash-back transactions at a merchant. Are there any specific considerations that should be given when the requirements for cash withdrawals apply to cash withdrawals via ATM and cash-back transactions at a merchant? (Chapter 7).

The Guidance provides useful clarification regarding the treatment of cash withdrawals, including ATM withdrawals and cash-back transactions. We nevertheless encourage FATF to consider extending the exception described in paragraph 209 to arrangements that provide an equivalent level of information sharing and control, such as ATM-pooling arrangements. In addition, the practical implementation of the proposed requirements will largely depend on the development of secure, automated, and standardised information-sharing mechanisms by card schemes, enabling financial institutions to exchange the required information efficiently and in compliance with applicable security, banking secrecy, and data protection requirements.

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

We welcome FATF’s payment-method-neutral approach and the guidance on instant payments, digital wallets, mobile money, and proxy identifiers. Additional clarification on instant-payment environments would be helpful, particularly regarding proxy identifier resolution and the balance between effective controls and payment efficiency. More broadly, Chapter 8 should remain principles-based, avoiding prescribed operational models and allowing flexibility to support innovation, interoperability, and consistent transparency outcomes across payment methods.

For virtual-asset transfers, further clarification would be welcome regarding alignment checks, interoperability between Travel Rule solutions, and the treatment of transactions received without the required Travel Rule information. Given the irreversible nature of blockchain transactions and the reliance on wallet addresses rather than verified beneficiary names, the Guidance could more explicitly recognise the role of pre-validation mechanisms and address operational challenges arising from fragmented Travel Rule infrastructures.

12) Is there any additional guidance that would address potential challenges in implementing Recommendation 16 with respect to data protection and privacy? (Chapter 9).

We welcome the inclusion of data protection and privacy considerations in Chapter 9. To support consistent implementation, the Guidance could further clarify that R.16 should be implemented in a manner consistent with applicable data protection frameworks. In particular, additional guidance would be welcome on the interaction between AML/CFT, sanctions, fraud-prevention, and payment-transparency objectives, as these activities may be subject to different legal bases, governance arrangements, and retention requirements. FATF could also clarify that compliance with legal and regulatory obligations constitutes an important basis for the processing of personal data in the context of R.16.

We also support the emphasis placed on the principle of data minimisation. Further clarification would be helpful to confirm that financial institutions are not expected to collect, retain, or process personal data beyond what is necessary to meet the objectives of Recommendation 16. In addition, FATF could recognise that certain measures envisaged by the Guidance, including holistic ongoing monitoring, alignment checks, profiling, and AI-based detection tools, may require specific governance arrangements and, in some jurisdictions, data protection impact assessments or additional safeguards.

Finally, additional clarity regarding responsibilities for data sharing across payment chains involving multiple financial institutions, PMIs, VASPs, and other participants would support more consistent implementation. This includes transparency obligations towards data subjects, the allocation of responsibilities where personal data is exchanged between multiple parties, and the challenges associated with cross-border data transfers in multi-jurisdictional payment arrangements. Clear, interoperable, and legally robust frameworks remain essential to support the collection, transmission, retention, and sharing of the information required under Recommendation 16.

We also welcome FATF's recognition that institutions may require an appropriate transition period to adapt their systems, processes, and governance arrangements to the revised requirements, given the legal, operational, and technical adjustments that may be required.

13) Are the three options for alignment check measures explained clearly enough for implementation? Are there any good practices that could be included in the Guidance as practical examples? Does the Guidance provide sufficient support for the proportionate implementation of alignment checks in jurisdictions where these may still be developing? (Chapter 10).

We welcome FATF's objective of reducing fraud and misdirected payments and support the flexibility provided through the different alignment-check options. In our view, the proposed approaches are sufficiently clear and allow implementation to be tailored to diverse payment systems, business models, and risk environments.

To maintain this flexibility, FATF could clarify that the three approaches are alternative implementation options rather than a hierarchical framework, allowing financial institutions to adopt the mechanism, or combination of mechanisms, most appropriate to their operational context and risk profile. The emphasis should remain on achieving effective fraud-prevention and payment-transparency outcomes rather than prescribing specific control models.

Additional practical examples illustrating the application of alignment checks across different payment environments would further support consistent implementation. The Guidance could also emphasise that alignment checks form part of a broader fraud and financial-crime control framework and do not replace the responsibility of payment service users to provide accurate beneficiary information.

Finally, FATF should avoid creating an expectation that alignment checks necessarily require real-time or pre-credit name-account matching. A risk-based approach should remain available, allowing institutions to combine pre-validation, post-validation, and ongoing monitoring measures as appropriate. Likewise, any mismatch identified through an alignment check should be considered a risk indicator requiring further assessment, rather than a conclusive indication of fraud or error.