20 August 2026

Comments of the European Banking Federation (EBF) on the draft Financial Action Task Force (FATF) Guidance on Recommendation 16.

Response to the FATF public consultation of June 2026 - deadline 21 August 2026

The European Banking Federation (EBF) welcomes the opportunity to comment on the draft Guidance on the implementation of Recommendation 16 (R.16), published for public consultation on 24 June 2026.

The EBF remains available to provide further input as this work progresses.

Introduction

The EBF supports FATF's objective of improving the transparency, traceability and integrity of cross-border payments and value transfers. Our comments focus on preserving effective financial crime outcomes while ensuring that implementation remains risk-based, proportionate, legally grounded and operationally achievable across diverse payment infrastructures, business models and jurisdictions.

In this context, we support the objective of revised R.16 to strengthen payment transparency and ensure that relevant originator and beneficiary information remains available throughout the payment or value transfer chain, in support of AML/CFT objectives as well as fraud prevention – including authorised push payment (APP) fraud, impersonation fraud, account takeover and the misuse of mule accounts. We welcome the clarity that the draft Guidance provides, in particular regarding the payment-chain concept and its application to an increasingly diverse payment landscape.

At the same time, implementation should remain practical, proportionate and aligned with the role of each participant in the payment chain. When complying with the travel rule, financial institutions should not be expected to obtain or verify information that is not available to them through their respective role, or otherwise be held responsible for matters beyond that role. The availability of additional R.16 data may support AML/CFT controls, investigations and risk assessment. However, the availability of such data should not, in itself, create broader AML/CFT monitoring obligations or imply that all additional R.16 data fields must be systematically assessed or used to generate alerts. The use of such information should remain targeted, risk-based and proportionate.

Accordingly, we recommend that the FATF:

- ensures consistent adoption of R.16 across jurisdictions, recognising the cross-border nature of payments and existing differences in regulatory implementation;

European Banking Federation aisbl
Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / mediacentre@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

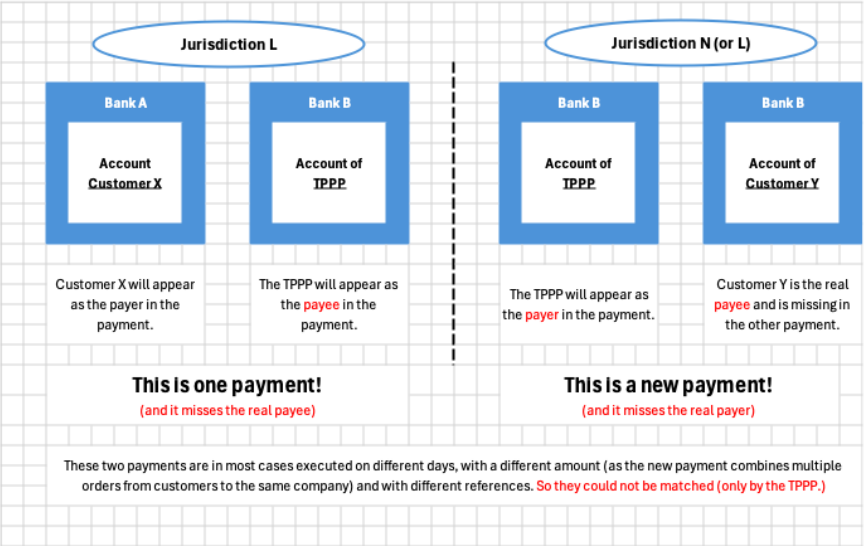
- preserves a risk-based, proportionate, technology-neutral and outcome-focused approach that recognises differences in payment infrastructures, business models and levels of market maturity
- avoids creating an expectation that financial institutions must proactively identify, retrieve or validate Legal Entity Identifiers beyond information already obtained and maintained through existing onboarding, customer due diligence and customer-information processes
- recognises that some implementation requirements depend on payment market infrastructure readiness, messaging standards, scheme rules and cross-industry data models, and may require realistic transition arrangements
- clarifies that mismatches should be treated as risk indicators rather than conclusive evidence of fraud or error
- ensures that implementation remains consistent with applicable data protection frameworks, including appropriate legal basis for the collection, transmission, retention and onward sharing of payment information across multi-jurisdictional payment chains
- encourages national legislators and the industry to pursue a phased approach or interim milestones, on a voluntary basis, to provide incentives and legal certainty for FIs and customers alike to adapt systems and processes in a gradual manner and to avoid the complexity and challenges of an implementation approach targeting a uniform fixed date.

Our detailed comments, structured by reference to the consultation questions, are set out below.

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

The scope of Recommendation 16 and the terminology used throughout the draft Guidance are, in general, sufficiently clear and provide a useful basis for implementation. Further clarifications would nevertheless be welcome, particularly in relation to VIBAN arrangements and cross-border cash withdrawals, as well as to illustrate how the Guidance applies to commonly used payment service providers (PSPs), third-party payment providers (TPPPs) and payment-facilitator models. In practice, a bank customer may pay a merchant through a TPPP, while the underlying transaction is split into separate settlement legs. Such arrangements are not sufficiently reflected in the current examples and may create uncertainty regarding the application of R.16 responsibilities.

We would also stress that these are not merely exceptional or low-volume scenarios. TPPP and payment-facilitator models may involve very high volumes of payments. Any ambiguity regarding the application of R.16 to the underlying payment and its separate settlement legs may therefore have significant implementation consequences when applied at scale.



Moreover, we have concerns that certain clarifications and interpretative elements go beyond the wording and intent of R.16 itself, by introducing more prescriptive expectations or, in some cases, overly permissive, particularly regarding

(i) the treatment of address information and the scope for using alternative location identifiers instead of the town name

(*please refer to question 4, point 2 below for further details*).

While additional guidance can support consistent implementation, some of these provisions may effectively create new operational requirements or additional risks that are not explicitly set out in R.16.

This approach risks reducing flexibility in the implementation of the Recommendation and may create significant operational challenges for financial institutions, particularly where the proposed measures require substantial adaptations to existing systems, processes, or data flows.

We therefore encourage FATF to ensure that the Guidance remains closely aligned with the principles and requirements set out in Recommendation 16, while preserving sufficient flexibility for jurisdictions and institutions to implement the standard in a risk-based and operationally feasible manner, without introducing undue leniency that could weaken the integrity of address-related information requirements.

(ii) the proposed implementation timeline. On the latter, the draft Guidance appears to move away from the timeline envisaged under the previous Interpretative Note towards an expectation of full implementation by 2030.

Such an approach may not sufficiently take into account the technical complexity of certain requirements, particularly alignment checks, nor the fact that important regulatory developments, including in the European Union, remain pending. In practice, full implementation by the date indicated may not be achievable for all

requirements, and institutions will necessarily need to prioritise certain measures and implement appropriate transitional arrangements.

We therefore encourage FATF to maintain flexibility regarding implementation timelines where significant legal and technical dependencies remain, allowing institutions to prioritise measures and apply appropriate transitional arrangements.

At the same time, we welcome the clarification provided in relation to footnote 49 through paragraphs 47 onwards, which supports a more consistent interpretation of the Recommendation.

Scope – payment transparency distinct from CDD (R.16 vs R.10). We also recommend that FATF clarify that R.16 payment-transparency obligations are distinct from, and should not be interpreted as creating, additional customer identification, verification or customer due diligence obligations beyond those already required under R.10. Several provisions referring to accuracy checks or verification could otherwise be read inconsistently across jurisdictions: further emphasis on this distinction would help ensure that supervisors do not interpret R.16 as expanding CDD obligations.

Terminology – "value transfer". We also recommend that FATF provide practical examples clarifying the term "value transfer" and how it applies across different operational scenarios, including where it differs, if at all, from a payment – for instance in account funding, securities-related transfers, and wallet-funding arrangements, where the movement of value between parties may be operationally indistinguishable from a payment transaction. The definition should remain sufficiently broad and technology-neutral to accommodate future payment and value-transfer models without requiring frequent updates to the Guidance.

With a view on any future development beyond the current scope of the guidance document: While agentic commerce/agentic payments is a nascent area of policy, FATF should consider addressing the potential use of AI agents to initiate payments and value transfers as being in scope. We don't expect FATF to be leading policy development in this area but there should be acknowledgement and coordination by national authorities to ensure the rules remain forward-looking.

Question 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).

Overall, the measures relating to the definition and functioning of the payment chain appear sufficiently clear.

The payment-chain concept is one of the strongest elements of the draft Guidance and provides much-needed clarity.

Further practical examples would nevertheless be useful for commonly used PSP and payment-facilitator models, where several technical or settlement legs may be involved in a single underlying customer payment. The Guidance should clarify where the R.16 payment chain starts and ends; which entity acts as ordering, intermediary or beneficiary financial institution; how responsibilities are allocated where the customer-facing entity differs from the account-servicing or payment-

executing entity; and how required R.16 information remains available where several payment infrastructures or settlement legs are involved.

Responsibilities should remain linked to the function performed by each participant and the information reasonably available to it.

Such examples could usefully cover open banking arrangements, embedded-finance models, digital wallets involving multiple regulated entities, hybrid fiat/virtual-asset payment chains, and platform-based payment arrangements, in order to clarify the notion of ordering financial institution and the distinction between obliged entities subject to R.16 and technical service providers that do not themselves qualify as financial institutions for these purposes.

We would also like to raise a point regarding paragraph 120, in order to avoid any interpretation that could imply an end-to-end responsibility for financial institutions where limitations arise from Payment Market Infrastructures (PMIs) or messaging standards.

Where end-to-end transmission is not technically feasible due to limitations of a PMI or messaging standard, individual financial institutions should not be held responsible for data loss, truncation or non-transmission over which they have no effective control.

In such cases, each financial institution should remain responsible for collecting, retaining and making available the required information within the scope of its own role and technical capabilities. In parallel, PMIs and standard-setting bodies should be encouraged to develop the technical capacity needed to support full end-to-end transmission of R.16 information.

In this respect, we would emphasise that PMIs are not merely technical channels: they define common rules, messaging standards, data formats and connectivity arrangements. FI compliance with R.16 should not be assessed without regard to these infrastructure-level constraints, which lie outside the control of individual financial institutions.

Domestic payments infrastructure used for cross-border payment chains. We welcome FATF's recognition that domestic payment infrastructures may increasingly be used to process parts of cross-border payment chains, and we would encourage further clarification of supervisory expectations where a financial institution or infrastructure does not have visibility of certain data elements, so that responsibilities remain proportionate, operationally achievable and aligned to the role performed in the payment chain.

Debit and pull-payment models. Further guidance would also be useful for debit-payment and payment-initiation models, including ACH-style, card-based and other pull-payment arrangements. In these models, the financial institution debiting the payer's account may not always be the party that receives the relevant payment instruction or has practical access to the beneficiary information needed to populate R.16 data. The Guidance should avoid a one-size-fits-all assumption that the payer's financial institution is always the operational starting point for R.16 data obligations, and should confirm that responsibilities remain allocated according to the role performed in the payment chain and the entity with practical access to the required data.

Question 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).

PMI-hosted data storage models may support payment transparency by reducing data-loss risks and facilitating retrieval of required R.16 information. At the same time, models in which the payment message contains only a token or reference to information stored elsewhere create important operational, AML/CFT, fraud and data-protection considerations.

While these emerging practices may offer certain operational benefits, relying on PMIs for the storage of required originator and beneficiary information would entail transmitting to them the full set of customer-related data needed by financial institutions to perform their AML/CFT and targeted financial sanctions (TFS) controls. Financial institutions must therefore retain effective and timely access to complete payment information and remain able to fulfil their regulatory obligations, including TFS screening, transaction monitoring, alignment checks, suspicious transaction reporting and fraud monitoring (e.g., detection of APP fraud, mule-account activity, account takeover and social-engineering scams or other suspicious payment patterns) and must remain able to evidence compliance vis-à-vis auditors and competent authorities.

At a minimum, if such models were to be contemplated, authorities should provide a clear governance framework defining the role and responsibilities of each actor, including PMIs and participating financial institutions. This framework should, in particular, clarify:

- The allocation of responsibilities for TFS screening
- AML/CFT controls
- Secure data storage, personal data protection, and the Conditions under which financial institutions can evidence compliance with their obligations
- Access rights and availability of the underlying information
- Retrieval times, particularly where controls must operate in real time
- Responsibilities for maintaining, validating and correcting stored information
- Auditability and traceability
- Operational resilience and dependency on the PMI
- Cross-border access and applicable data-protection requirements
- Common industry standards for data fields, reference formats and access protocols across participating PMIs and financial institutions, to avoid fragmentation and ensure that token-reference models support, rather than weaken, end-to-end payment transparency.

At the same time, the availability of additional R.16 information should not imply that all such data must systematically be used for AML/CFT monitoring or alert generation. Its use should remain risk-based, targeted and proportionate.

More generally, we consider that token- or reference-based models should only be regarded as compatible with R.16 only where the complete underlying information remains readily retrievable and accessible to financial institutions and competent authorities, supports timely sanctions screening and transaction monitoring, and preserves traceability, auditability and an immutable audit trail throughout the lifecycle of the transaction.

Question 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).

The draft Guidance generally provides clarity regarding the information requirements applicable to cross-border payments and value transfers, as well as the circumstances in which origin of funds information should be transmitted.

However, we are concerned that certain provisions of the Guidance appear to go beyond the requirements set out in Recommendation 16 itself and may create unintended challenges, as explained below. Accordingly, we would appreciate clarification on the following concerns.

1) About the de minimis threshold (paragraphs 176 and 177)

Recommendation 16 (R.16) and its interpretative note (INR.16) set up a de minimis threshold under which it is not required to transmit some payment information. The implementation of such a threshold is clearly left to the discretion of jurisdictions (cf. paragraphs 8 and 10 of INR.16: "Countries may also adopt a de minimis threshold"). The Guidance appears to go beyond R.16 and INR.16 by quasi-requiring the application of a de minimis threshold (cf. paragraph 176). While we acknowledge the rationale underpinning the proposed threshold, in particular its relevance to financial inclusion and lower-value payments or value transfers, we strongly recommend preserving flexibility for jurisdictions to determine whether and how such thresholds should be applied.

More specifically, the implementation of such a threshold would undermine the capacity of obliged entities to implement TFS which apply irrespective of the amount of the payment or value transfer, which constitutes one of the objectives of R.16 as per paragraph 16 (c) of the Guidance: indeed, as key information would be missing, potential designated persons and entities could remain unidentified. The implementation of such a threshold could therefore create major financial crime risks that obliged entities would not be able to mitigate or manage effectively.

Where jurisdictions choose to implement a de minimis threshold, further clarification would nevertheless be beneficial regarding

- The interaction between de minimis thresholds and existing regional frameworks, particularly within the EEA.
- The treatment of linked transfers for threshold purposes.
- The application of thresholds to transactions denominated in currencies other than EUR/USD.
- The statement "financial institutions would be expected to adopt practices that meet the most stringent requirements likely to apply": Clarification is needed on the reference point — e.g., the most stringent requirement

across all jurisdictions in which an FI operates, or those relevant to a given transaction — as an undifferentiated "highest standard" approach could prove disproportionate. Clarification would also be welcome on what harmonizing thresholds means in practice — in particular, whether it implies a single common threshold, harmonization to the lowest applicable level, or alignment across transaction types, and how this would accommodate differing jurisdictional risk profiles.

In conclusion, we consider that the approach set out in the draft Guidance goes beyond the wording of R.16 and may undermine the implementation of more transparency in payments with a negative impact on fraud detection with only partial pre-alignment checks, on AML/CFT and TFS due to the lack of key information.

In this context, FATF could also consider publishing an implementation annex mapping R.16 information requirements to the relevant ISO 20022 message fields, in order to promote interoperability, support consistent implementation across jurisdictions and PMIs, and reduce technical uncertainty for financial institutions.

2) Three-business-day information retrieval and origin-of-funds requirements

Further practical guidance would also be useful on how the three-business-day information retrieval requirement should operate in practice and on the application of origin-of-funds requirements to PSPs, wallets and other modern payment models.

For origin-of-funds requirements in particular, practical end-to-end examples would be useful to illustrate how the requirements apply where different institutions perform customer interaction, account servicing and payment execution functions.

The Guidance should also maintain a clear distinction between the responsibilities of the ordering institution and those of downstream institutions. Receiving institutions should not be expected to verify information that lies outside their role or to establish whether additional information might have been available to another institution in the payment chain.

3) About alternative data (paragraphs 142 and 143)

The use of alternative data to the address often prevents systematic monitoring by replacing geographic information with non-systematically leverageable information such as the client identification number, which creates risk and additional workload/friction. As for alternative data possible for accounts, these prevent the systematic alignment check by providing non standardised customer identification. Both in light of Sanctions and Fraud requirements, the risk and additional cost implied is deemed too high not to require payment transparency information for cross border payments notwithstanding the amount nor the use of alternatives.

As for the possible alternatives to town name, we understand the objective of the FATF for more inclusion, but we firmly believe this should not be at the expense of an efficient and secure environment. While the existence of an address in a

structured format might vary from one location to another, information about a town or village seems highly achievable. Accordingly, a nearest alternative to a town name which can be something not providing enough details or specificity of its geographical location could mislead the filtering and shall not be permitted.

At the same time, we recognise the financial inclusion objectives underpinning the use of alternative information and fallback options where standard address information is unavailable. These flexibilities are important in jurisdictions or customer contexts where standardised address information may not be available. Alternative information should, to the greatest extent possible, preserve the ability of financial institutions to perform sanctions screening, transaction monitoring, fraud detection and alignment checks, and should therefore remain sufficiently standardised, structured and interoperable to support effective downstream controls and avoid creating unnecessary operational complexity or weakening payment-transparency outcomes.

4) About the debtor bank's responsibility regarding the LEI (paragraph 151)

While we welcome the clarifications provided in relation to the Legal Entity Identifier (LEI), in particular regarding the relevance of the BIC code, paragraph 151 may be misleading. It could be interpreted as requiring originating banks to take on additional responsibilities not provided for in Recommendation 16 or its Interpretative Note, by requiring them to actively retrieve the LEI where they reasonably ascertain that one exists, even where it has not previously been obtained. To avoid such interpretation, we recommend replacing the wording "asking the originator" in paragraph 151 with "when provided by the originator", in order to make clear that the originating bank should transmit the LEI where it has been provided or obtained, but should not be subject to an additional obligation to request or retrieve it specifically for the purposes of Recommendation 16.

The LEI is one piece of key information among other information collected, verified and monitored as part of the bank's customer due diligence framework. Its timeliness and accuracy should therefore be ensured through the appropriate CDD mechanisms and should not be subject to additional requirements arising from Recommendation 16. This clarification would also ensure that the Guidance remains aligned with the existing CDD-based approach, under which the LEI may be used where available, without creating a separate obligation for payment purposes.

5) About the LEI as an alternative data point

We would also like to draw FATF's attention to the complexity of relying on the LEI as an alternative data point for geographic assessment purposes. The LEI is designed around a legal-entity-centric view, which may result in international branches being mapped to a single parent LEI code. This approach does not necessarily reflect the geographical reach or location relevant to a specific transaction.

Accordingly, the LEI may not be suitable for determining the geographical location or reach of a transaction. It should only be used in specific cases as a complementary cross-checking tool and should not replace more precise and transaction-relevant geographic information.

6) About the debtor and creditor full-name requirement

We welcome the alignment of Recommendation 16 with Regulation (EU) 2023/1113 regarding the requirement to transmit the full name of the debtor and creditor, whereas the previous formulation only referred to the name. However, to avoid any ambiguity, in particular in light of paragraph 129, the Guidance should make clear that initials or truncated names should not be considered sufficient.

At the same time, we recognise that technical constraints may arise in limited circumstances, including name truncation in legacy messaging or infrastructure environments. In such cases, we recommend that FATF clarify that any truncation or abbreviation should not materially impair the ability of downstream financial institutions to identify the relevant customer or perform effective sanctions screening, transaction monitoring and payment-transparency controls.

Even where there is no ambiguity for the financial institution onboarding the client, the beneficiary financial institution will generally not have access to the full customer KYC file. The full name, as stated in the official document collected as part of customer due diligence, should therefore be transmitted throughout the entire payment chain.

7) About the "Ultimate Debtor" and "Ultimate Creditor" fields

We would welcome a specific clarification regarding FATF's expectations in relation to the "ultimate debtor" and "ultimate creditor" fields referred to in the draft Guidance. In particular, it would be helpful if FATF could clarify whether, and to what extent, financial institutions are expected to screen or otherwise perform controls on this information.

Question 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 flexible approach for situations where formal address documentation is unavailable, particularly from a financial-inclusion perspective.

For existing customers, verification of originator address information is generally feasible, as address information forms part of AML/CFT onboarding requirements and ongoing CDD processes.

Hence, this requirement to verify the accuracy of the originator's address should only apply where the institution holds a customer relationship with the originator and has access to the underlying KYC information. It should not be interpreted as requiring beneficiary institutions to independently verify originator information on a transaction-by-transaction basis.

Indeed, the feasibility of verifying the originator's address depends significantly on the role of the financial institution in the payment chain.

Where the financial institution acts as the originator's payment service provider, the originator's address is typically collected and verified as part of the customer due diligence measures applied at onboarding and throughout the business relationship. In this context, the institution can rely on its KYC framework, including customer identification and periodic reviews of customer information, to ensure that the address information is accurate and up to date. Such consultation is often performed manually and entails significant operational effort. It can therefore only be implemented in a proportionate manner in respect of the institution's own customers and within the context of customer due diligence obligations.

By contrast, where the financial institution acts as the beneficiary's payment service provider, it generally has no customer relationship with the originator. In such circumstances, the beneficiary's payment service provider cannot carry out any verification of the originator's address.

While ad hoc verification could theoretically be performed in individual cases, this would only be proportionate where specific risk indicators, inconsistencies or suspicions have been identified. Requiring beneficiary institutions to verify the accuracy of the originator's address for all cross-border payments or value transfers above the de minimis threshold would be unrealistic and disproportionate, given the volume of transactions involved and the absence of a direct relationship with the originator.

We therefore consider that, in the absence of risk indicators suggesting that the information may be inaccurate, beneficiary institutions should be entitled to rely on the payment information transmitted through the payment chain and should not be expected to independently verify the originator's address. The Guidelines should clarify this point to avoid creating an obligation that is impracticable to implement in practice and should provide further clarification on the role of PSPs in the payment chain, as the role performed by a PSP directly affects the practical feasibility of address verification.

Consistent with footnote 49, we would also welcome confirmation that the Guidance does not prescribe a specific verification methodology: different verification mechanisms may be appropriate depending on the product, business model, customer relationship, payment model and risk context.

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

We welcome the additional clarity and practical support provided by the Guidance for implementation in lower-capacity contexts.

In particular, the recognition of year of birth and country/town information as valid fallback options provides useful implementation certainty and supports financial inclusion.

The Guidance should make clear that information provided in accordance with these permitted fallback options constitutes valid R.16-compliant information.

An intermediary or beneficiary Financial Institution (FI) generally cannot determine whether a complete address or full date of birth was available to the ordering FI. Receiving institutions should therefore be able to rely on permitted fallback information and should not be expected to assess whether more detailed information could have been obtained upstream.

This would support consistent implementation and help avoid unnecessary payment friction.

This could usefully be illustrated with examples drawn from jurisdictions with limited civil registries, mobile-money ecosystems, domestic payment switches, agent-based financial services, and other contexts in which reliable address infrastructure is not uniformly available.

Question 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).

The draft Guidance provides useful clarification regarding the measures that may support compliance with the requirement that account numbers should not be used to disguise the identification of the country where the financial institution servicing the account resides.

However, we consider that further clarification would be useful, in particular regarding the allocation of responsibility and the interaction with existing or upcoming regulatory frameworks.

1) About the responsibility for virtual IBANs

Several of the proposed measures would be difficult to implement for institutions other than the one issuing the virtual account: ordering institutions generally receive beneficiary information from the payer and are not required to verify it. In many cases, they may therefore not be able to determine whether a virtual account number is being used.

We recommend that the Guidance expressly confirm, consistent with the wording of Recommendation 16 and paragraph 162 of the draft Guidance, that the responsibility to ensure that account numbers are not used to disguise the identification of the country rests with the institution that owns the master account and services the virtual IBAN, which alone has the necessary visibility over the account structure and underlying relationships. Indeed, in practice, other financial institutions in the payment chain may not be in a position to identify the underlying master account or to determine how the virtual IBAN has been structured. Placing such responsibility on institutions that do not own the master account or do not service the virtual IBAN would therefore be operationally unrealistic and could create expectations that cannot be effectively implemented.

The primary responsibility should therefore rest with the institution issuing the virtual account number, as that institution has the necessary visibility over the account structure, end users and underlying account relationships.

2) About existing regulatory developments on virtual IBANs

We understand the FATF's position set out in paragraph 164 that "Greater transparency in the use of virtual account numbers could also be achieved through amendments to the relevant standards, for example, adding a prefix to virtual account numbers".

However, it should be noted that local and regional regulatory frameworks are already progressing in this area: for example, under Directive (EU) 2024/1640 (AMLD6), Member States are required to maintain national centralised automated mechanisms enabling the identification of bank accounts, including virtual IBANs, and their holders. These national mechanisms are to be interconnected at Union level through the Bank Account Registers Interconnection System (BARIS). Data retention itself, however, remains governed at national level.

Against this background, we encourage FATF to ensure that the Guidance remains sufficiently flexible to take into account existing and future regional regulatory solutions (including registries and look-up services), rather than prescribing a single technical approach where jurisdictions have already adopted, or are in the process of developing, mechanisms designed to achieve the same transparency objective.

We also recommend that the Guidance continue to emphasise that virtual account number arrangements should not be used in a manner that obscures the cross-border nature of an underlying banking relationship or causes a transaction to appear domestic where the relevant servicing arrangement is cross-border. While legitimate treasury, liquidity management and reconciliation structures should remain fully supported, the key objective should remain that the account-servicing financial institution and the applicable jurisdiction can be reliably identified by the relevant participants and competent authorities.

This issue is also relevant to APP fraud prevention, where transparency of the ultimate beneficiary relationship is an important risk-mitigating factor: we would welcome further examples of how PSPs can maintain such transparency while supporting innovative payment models.

Question 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).

The draft Guidance does not provide any explanation regarding the role of certain participants, such as payment service providers other than acquiring banks or marketplaces, despite their key role in payment transactions. We would also note that certain actors, such as marketplaces, and certain values, such as quasi-cash, are not clearly addressed or defined under R.16, and would welcome clarification from FATF as to whether, and in what capacity, such actors and values fall within the scope of the Recommendation's requirements.

While the role of payment aggregators/facilitators is referred to several times (paragraphs 188 and 192, footnotes 46–47), the term is not defined in the

Guidance. We would welcome the inclusion of a specific definition for these types of actors. We would also draw attention to the operational challenges in identifying sponsored issuers: the information available differs by card network (for instance, Visa provides the BIN but not the sponsored entity's name, requiring additional research, whereas Mastercard generally provides both, though BIN allocations may be reassigned to another entity over time), and the name of the sponsored entity may vary across card networks, as each uses its own terminology. This lack of uniformity also complicates communication with sponsored entities.

Overall, these challenges could hinder the effective implementation of TFS, as the identification of the sponsored entity is often necessary to block a transaction.

Separately, we support the differentiated, more limited regime provided for in the Guidance, under which the card number accompanies the transaction, while the name and location of the issuing and acquiring financial institutions are available upon request.

We would welcome clarification that banks and card-chain parties are expected to be able to provide such information on request, without this necessarily implying it must accompany every card payment by default.

More broadly, implementation in card ecosystems should, where possible, leverage existing standardised and secure infrastructures, avoiding unnecessary duplication of information already available.

This could help limit unnecessary processing of card-payment data while preserving access to relevant information where specific AML/CFT risk indicators or investigative needs arise.

Question 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).

We would welcome additional examples illustrating what should be considered a purchase of goods or services, in particular for scenarios not currently addressed in the draft Guidance, such as donations to charities and quasi-cash transactions (e.g., purchase of casino chips, acquisition of crypto-assets, or deposits to gambling websites). Further examples covering these scenarios, together with a more precise definition of "goods" and "services" (including a clearer explanation of what falls within their scope) would help institutions apply the applicable regime consistently and ensure the appropriate information is collected and transmitted.

Question 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 draft Guidance provides useful clarifications regarding the scope of information requirements applicable to cash withdrawals, including cash withdrawals via ATM and cash-back transactions at a merchant.

However, we consider that further clarification would be useful to ensure that the proposed requirements can be implemented in an operationally feasible and proportionate manner, in particular where several actors are involved in the processing of the transaction.

1) About the same-institution exception for cash withdrawals

We welcome the clarification of the same-institution exception for cross-border cash withdrawals in paragraph 209 of the draft Guidance. We consider, however, that this exception should not be limited to situations involving a capitalistic relationship (e.g., parent-subsidiary): in certain cases, joint operational arrangements may allow financial institutions to reach the same level of information and control, even in the absence of such a capitalistic link.

In line with the "same risk, same principle" approach, we therefore recommend that the exception described in paragraph 209 be extended to include "entities pooling ATMs for financial institutions".

2) About the dependence on card scheme solutions

We fully understand the need to provide relevant information in the context of cash withdrawals and remain available to support the exchange of such information where appropriate.

However, the practical implementation of these requirements will strongly depend on the ability of card schemes to develop dedicated tools and processes, including:

- mechanisms to ensure that information requests are appropriate and legitimate, and to prevent fraud or phishing attempts.
- a secure channel and environment for the exchange of information, taking into account applicable requirements, including PCI DSS standards, banking secrecy and data protection rules.
- the ability to transmit detokenised or de-PANised information allowing the identification of the card owner where necessary.
- automated, fluid processes capable of handling anticipated volumes, from the initial request through identification of the issuing bank by the scheme to a response within three working days.

More generally, we consider that any assessment of a financial institution's compliance in this context should take into account the operational role played by card schemes and PMIs, as well as the actual availability of secure channels and data-sharing arrangements compliant with applicable privacy and security requirements.

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

Chapter 8 provides useful clarification, particularly for instant payments. Nevertheless, additional guidance would be useful for increasingly complex payment arrangements involving payment facilitators, wallet providers, embedded-finance arrangements, marketplace payment models, virtual-account structures, and scenarios where customer interaction, onboarding, transaction

initiation, account provision and payment execution are performed by different institutions. The Guidance should clarify how R.16 responsibilities are allocated where the customer-facing provider does not itself execute the payment. Intermediary institutions should not be expected to obtain or verify information not available to them through their role in the payment chain.

1) Adaptation of alignment checks to virtual-asset transfers.

The proposed alignment-check framework may require some further adaptation to reflect the specific features of virtual-asset transfers. Unlike traditional payment messages, an on-chain transaction generally includes a wallet address, but not the verified name of the beneficiary. As a result, comparing the beneficiary's name transmitted through a Travel Rule solution with the wallet address recorded on-chain is not, in itself, sufficient to establish alignment. A wallet address is a technical identifier and does not, by its nature, contain or evidence the identity of the person controlling it. Transaction-level alignment checks may be feasible where the beneficiary VASP maintains a reliable and sufficiently direct mapping between the destination wallet address and a customer whose identity has been verified. However, their effectiveness may be limited where addresses are dynamically generated, changed or rotated, managed through omnibus arrangements, or otherwise not clearly and unambiguously associated with an individual customer in the beneficiary VASP's systems. Similar limitations may arise in relation to holistic ongoing monitoring based on misalignment. While a custodial VASP may take into account inconsistencies between Travel Rule information and its customer records as part of its broader transaction-monitoring framework, misalignment cannot readily constitute a meaningful indicator where the required Travel Rule information has not been received or where there is no reliable reference dataset against which the beneficiary's name and wallet address can be compared. In this context, pre-validation appears to be the most suitable and effective alignment mechanism for VASP-to-VASP transfers. Such a mechanism could enable the ordering VASP, before executing an irreversible on-chain transfer, to confirm with the beneficiary VASP that:

a. the destination wallet address is controlled or serviced by the beneficiary VASP;
b. the address is associated with the intended beneficiary;
c. the beneficiary information transmitted through the Travel Rule solution is sufficiently consistent with the information held by the beneficiary VASP; and
d. the beneficiary VASP is able to receive the required Travel Rule information through an appropriate and secure communication channel.

This approach would be consistent with the instantaneous and generally irreversible nature of virtual-asset transfers, where a post-transaction alignment check may occur too late to prevent crypto-assets from being made available to an unintended beneficiary. The Guidance should therefore recognise pre-validation as generally well-suited to VASP-to-VASP transfers, given the structural limitations of post-transaction and holistic-monitoring approaches described above, while remaining technology-neutral as to the specific mechanism used and allowing alternative approaches where they can demonstrably deliver an equivalent preventive outcome. However, this should not be interpreted as extending a

comparable expectation to other payment types, business models or jurisdictions where the same structural limitations do not apply.

2) Operability of Travel Rule solutions for VASPs

Under the Travel Rule, the relevant originator and beneficiary information is generally transmitted separately from the on-chain transaction. The effectiveness of the framework therefore depends on the ability of the ordering and beneficiary VASPs to reliably identify each other and exchange the required information through appropriate and secure channels. In practice, VASPs may rely on different Travel Rule solutions, networks or communication protocols. Where such solutions are fragmented or not interoperable, an ordering VASP may be unable to:

a. identify the Travel Rule solution used by the beneficiary VASP;
b. determine whether the beneficiary VASP can be reached through that solution;
c. authenticate the beneficiary VASP;
d. securely transmit the required information;
e. obtain confirmation that the information has been duly received; or
f. perform pre-validation before executing the on-chain transfer.

Similarly, the beneficiary VASP may receive crypto-assets without receiving the corresponding Travel Rule information, even where the ordering VASP has attempted to comply using a different technical solution. This creates a broader risk of fragmentation in the transmission of originator and beneficiary information and may undermine the payment-transparency objective of the Travel Rule. FATF should therefore consider establishing a clear interoperability principle for Travel Rule solutions used within the same payment scheme. We recommend that the FATF Guidance:

a. address interoperability as a core component of effective Travel Rule implementation;
b. encourage interoperability between different Travel Rule solutions, while remaining technologically and commercially neutral;
c. clarify the responsibilities of the ordering VASP where the beneficiary VASP cannot be reached through its Travel Rule solution;
d. clarify whether a transfer may proceed where the required information cannot be transmitted before execution due to a lack of interoperability.

3) Crypto-assets received without prior notification or Travel Rule information.

Unlike many traditional payment arrangements, a beneficiary VASP may have no technical means to prevent a third party from initiating an on-chain transfer to an address that has been published, disclosed or previously allocated to a customer. By the time the beneficiary VASP identifies the transfer, the transaction may already have been confirmed on the blockchain and, in practice, cannot generally be suspended or rejected at protocol level. FATF should therefore clarify the responsibilities of a beneficiary VASP where crypto-assets are received without the required Travel Rule information, in particular where the beneficiary VASP is unable to identify any regulated institution behind the originating wallet address. In particular, the Guidance should clarify:

a. whether the assets should be placed on hold at customer-account level pending further investigation, even where the underlying blockchain transaction cannot itself be suspended or rejected;
b. what reasonable steps the beneficiary VASP is expected to take to identify the originator and assess whether the originating address is controlled by another VASP;
c. what measures are expected where no originating VASP can be identified or contacted;
d. for how long the beneficiary VASP should seek to obtain the missing information before deciding whether the assets may be credited, restricted, returned or otherwise dealt with;
e. whether returning the assets to the originating address would be appropriate, taking into account that such address may not reliably identify the original sender and may be associated with heightened sanctions, fraud or money-laundering risks.

4) Payment transparency and fraud prevention

Payment transparency is also relevant to fraud prevention across instant payments, digital wallets and mobile payment solutions. The speed and practical irreversibility of modern payment methods increase the importance of ensuring that R.16 information can be used in a timely manner to support real-time fraud controls and risk assessments. Additional examples showing how payment transparency data may support fraud detection and intervention in instant-payment environments would therefore be useful.

At the same time, the availability of additional structured payment information should not imply that all data fields must systematically be used for AML/CFT monitoring or alert generation. Such use should remain risk-based, proportionate and relevant to the identified ML/TF risk.

More generally, we recommend that the Guidance remain focused on the functions performed and risks presented, rather than on legal forms or product categories, in order to preserve technological neutrality with respect to open banking, embedded finance, corporate treasury arrangements, multi-wallet ecosystems, proxy identifiers and cross-border wallet-to-wallet transfers.

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

The draft Guidance provides useful clarification on the data protection and privacy considerations that may arise in the context of the implementation of Recommendation 16.

However, we consider that further guidance would be useful to ensure that the implementation of R.16 remains consistent with applicable data protection frameworks, in particular where payment transparency requirements involve the collection, transmission, retention and further processing of personal data by actors in the payment chain.

1) **About the definition of fraud and its interaction with AML/CFT objectives**

We welcome the explicit inclusion of fraud prevention among the objectives of Recommendation 16. However, the Guidance should further clarify how fraud prevention objectives interact with AML/CFT objectives under R.16.

Indeed, under data protection frameworks, fraud prevention and AML/CFT monitoring are generally considered as separate processing activities, with distinct purposes and, in some cases, different legal bases, governance arrangements and retention requirements. Greater clarity on the relationship between these processing activities would therefore be beneficial.

In addition, the Guidance would benefit from defining the concept of "fraud" or at least providing illustrations of the fraud typologies falling within the scope of R.16, in order to support a consistent interpretation and implementation across jurisdictions.

We also recommend that FATF clarify the distinction between fraud and misdirected payments. While fraud can result in a payment being misdirected, misdirection may also arise from non-malicious customer error, inaccurate beneficiary information, or operational issues. Clearer terminology would help financial institutions apply proportionate controls, avoid treating every instance of misdirection as a fraud event, and distinguish between fraud prevention, error-resolution and payment-transparency obligations.

2) **About data protection impact assessments and retention periods**

The Guidance should provide further clarification regarding data protection impact assessments and data retention periods. In particular, it should acknowledge that certain processing activities envisaged under R.16, such as holistic ongoing monitoring frameworks, profiling or AI-based detection tools, may require a data protection impact assessment under applicable data protection laws.

Providing such clarification would help regulated entities define the appropriate governance, while ensuring that data retention periods remain proportionate to the purposes pursued and aligned with applicable legal requirements.

3) **About the legal basis for processing under R.16 and the EU AML Regulation (AMLR)**

Based on the wording of paragraph 240 of the draft Guidance, we understand that the envisaged legal basis may be the performance of a task carried out in the public interest. However, while AML/CFT objectives serve an important public interest, in some Member states, private entities cannot generally rely on this legal basis under applicable data protection frameworks.

In the European Union, the most appropriate legal basis for processing personal data in this context would appear to be compliance with a legal obligation, in particular under the EU AML Regulation (AMLR) and related AML/CFT requirements.

4) **About data minimisation**

We support the reminder in paragraph 241 that the principle of data minimisation should apply to the processing of personal data under R.16. It is important to ensure that all categories of personal data necessary for the fulfilment of AML/CFT

obligations are clearly identified and documented, as only those data that are strictly necessary for such purposes should be collected and processed.

5) About transparency obligations

The transparency section in paragraph 245 would benefit from a clearer distinction between general transparency obligations and individual information obligations. While general information may be provided through privacy notices, AML/CFT disclosures or public policies, additional guidance is needed regarding the provision of individual information to data subjects in the context of payment transactions.

In particular, the Guidance should clarify which participant in the payment chain is responsible for informing the payer and the beneficiary about the processing of their personal data, especially where personal data is transmitted between multiple ordering, intermediary and beneficiary financial institutions.

The Guidance should also address the application of the indirect collection exemption under applicable data protection frameworks where a financial institution receives personal data from another participant in the payment chain rather than directly from the data subject.

6) About the transition period

We welcome the recognition in paragraph 248 that regulated entities may require a transition period to adapt their systems, processes and governance arrangements to the revised requirements. However, it should be expressly specified that regulated entities should not be subject to sanctions during this transitional period.

Such clarification would support a proportionate implementation approach and avoid penalising institutions while significant legal, technical and operational adjustments are still being implemented.

7) About personal data transfers outside the European Union

The wording proposed in paragraph 250 may create confusion between the legal basis for processing personal data and the derogation allowing the transfer of personal data outside the European Union. Under the European General Data Protection Regulation (GDPR), the legal basis for processing and the conditions for international transfers are distinct requirements.

In particular, Article 49 GDPR provides that a transfer may take place, even in the absence of an adequacy decision or appropriate safeguards, where the transfer is necessary for important reasons of public interest. The Guidance should therefore clarify this distinction to avoid any misunderstanding regarding the conditions under which personal data may be processed and transferred in the context of R.16.

8) About holistic ongoing monitoring, pre-alignment checks and automated decision-making

In general, FATF should acknowledge that different, risk-based implementations are valid, and allow jurisdictions flexibility to determine the appropriate balance of controls. Emphasis should be on results and outcomes rather than the

prescribed "how" – particularly as criminals will study requirements closely and adapt their tactics to circumvent them.

Holistic ongoing monitoring (HOM) is the most flexible approach in this regard, spanning detective, preventive, and responsive measures. Assessment should focus on the outcome it delivers — the reduction in fraud and other illicit activities – rather than on the specific means of achieving it.

To that end, the interaction between holistic ongoing monitoring frameworks, alignment-check mechanisms and Article 22 GDPR warrants further clarification. In particular, the Guidance should identify and address the exemption that may permit automated decision-making in this context.

Depending on the circumstances, this could involve either relying on the contractual necessity exemption, where such an interpretation is accepted under the applicable legal framework and following appropriate dialogue with data protection authorities, or encouraging national legislators to provide for an explicit legal authorisation, accompanied by suitable safeguards for data subjects.

This issue is particularly important as certain outcomes resulting from fraud detection, AML/CFT controls or alignment-check mechanisms, such as the suspension, postponement or rejection of a payment transaction, may constitute decisions producing legal or similarly significant effects on individuals within the meaning of Article 22 GDPR. The Guidance should therefore provide greater clarity on the conditions under which such processing activities may be implemented and on the safeguards that should apply.

Finally, paragraph 267 appears to be inconsistent with the beginning of the section, which states that only the categories of data listed in Chapter 5 may be collected and processed. Behavioural indicators, historical transaction patterns or, in some cases, network-wide information do not appear to be included in that chapter. The Guidance should therefore clarify whether such data may be processed for holistic ongoing monitoring or alignment-check purposes, and if so, under which legal basis, safeguards and data minimisation requirements.

9) About the practical implementation of "availability by other means"

Further guidance would also be beneficial regarding:

- the practical implementation of "availability by other means" arrangements;
- governance arrangements where information is stored centrally or made available through shared infrastructures;
- responsibilities where information requested under R.16 cannot ultimately be provided;
- how retrieval obligations should be balanced against local data-protection restrictions in cross-border scenarios;
- which institution bears responsibility in such circumstances; and
- what constitutes reasonable efforts to obtain the information.

R.16 data should be processed in accordance with applicable data-protection principles, including lawfulness, data minimisation, proportionality, accuracy, auditability and security.

The availability of additional R.16 data may support AML/CFT effectiveness where it is risk-relevant, but should not result in indiscriminate data collection, broader supervisory expectations or disproportionate processing. Its use should remain risk-based and proportionate to the relevant payment context and identified ML/TF risks.

The Guidance should therefore distinguish between information required for payment transparency and traceability and information that may, depending on the risk context, support AML/CFT-related controls.

Cross-border data-sharing in multi-jurisdictional payment chains. We also recommend that FATF acknowledge the cross-border data-sharing challenges that may arise where R.16 information is transmitted through multi-jurisdictional payment chains. The Guidance should encourage jurisdictions to ensure that AML/CFT, sanctions and payment-transparency obligations are supported by clear and compatible legal bases for the collection, transmission, retention and onward sharing of required payment information, including where data is exchanged between financial institutions, PMIs and competent authorities.

In this context, we would also recommend that the Guidance address the need for cooperation between AML/CFT and data-protection authorities, the development of international recognition mechanisms and harmonised approaches to cross-border data transfers, and practical guidance on the use of Privacy Enhancing Technologies, appropriate retention periods, and the interaction between R.16 and the GDPR.

Question 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 the three options for alignment checks and the overall risk-based framework. However, we consider that:

- Alignment-check requirements should remain risk-based, proportionate and technology-neutral;
- Institutions should retain sufficient flexibility to adopt different implementation approaches, reflecting their risk profiles and operational models;
- In certain cases, post-payment monitoring, exception handling and risk-based fraud controls may prove more effective and operationally practical than introducing pre-transaction friction.

We recommend that FATF clarify that beneficiary alignment measures may be implemented through a range of risk-based approaches, and that no single alignment-check method should be viewed as inherently superior in all circumstances. The appropriateness of a particular approach will depend on the payment rail, participant access to relevant information, payment market infrastructure capabilities, legal framework, and risk profile of the underlying transaction.

FATF may also wish to acknowledge that, in certain payment environments, including some VASP-to-VASP transfer models where transactions may settle

rapidly and be difficult to reverse once completed, pre-validation measures can provide an effective risk mitigation tool. However, such recognition should not be interpreted as establishing a hierarchy of controls or a supervisory expectation that pre-validation must be adopted across all payment types, business models, or jurisdictions.

Ongoing or post-validation alignment checks performed by the beneficiary PSP may also appear to provide a suitable assessment of any potential mismatches between the actual and intended payee.

Institutions should retain the flexibility to implement alignment controls that are appropriate to their specific risk environment, provided those controls effectively address the risk of misdirected transfers and support the objectives of Recommendation 16.

Further practical guidance would be useful on: what constitutes a reasonable degree of alignment and acceptable mismatch tolerances, the treatment of acceptable variations and legitimate differences; the interaction between pre-validation, post-validation and holistic monitoring approaches; and implementation where counterparties or jurisdictions do not support pre-validation mechanisms.

Alignment checks can also serve as an important fraud-detection mechanism: a mismatch may indicate identity misuse, account takeover, mule-account activity, other payment fraud or an operational error. A mismatch should not, however, automatically trigger AML/CFT measures. Banks may need to assess, on a risk-based basis, whether a mismatch is primarily operational or fraud-related and whether the circumstances warrant AML/CFT-related follow-up.

The Guidance should therefore further clarify when misalignment may justify enhanced due diligence or consideration of suspicious transaction reporting, while avoiding any implication that every mismatch requires AML/CFT measures.

We also recommend that FATF clarify that alignment checks do not alter the fundamental principle that the originator remains responsible for providing accurate beneficiary details and authorising the payment. Alignment checks should be viewed as an additional fraud-mitigation tool, not as a substitute for the originator's responsibility, nor as transferring responsibility for payment-initiation accuracy from the originator to the beneficiary institution.

More generally, the Guidance should maintain a clear distinction between payment-transparency controls, fraud-prevention measures and AML/CFT controls, given their different objectives and operational consequence.