Consultation Response

AFME Response to FATF's Consultation on the Draft Guidance to Recommendation 16 (Payment Transparency)

21/08/2026

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to comment on FATF's draft guidance to Recommendation 16 (R.16) which is open for consultation. The Association for Financial Markets in Europe (AFME) is the voice of the leading banks in Europe's financial markets, providing expertise across a broad range of regulatory and capital markets issues. We represent over 150 leading global and European banks and other significant market players. Our members play a vital role in Europe's financial ecosystem, underwriting around 90% of European corporate and sovereign debt, and 85% of European listed equity capital issuances. Importantly, AFME members are market makers, providing liquidity, which is essential for ensuring financial markets can function efficiently. We also represent law firms and other associate members which advise market participants and support AFME's legal and regulatory initiatives.

AFME is registered on the EU Transparency Register, registration number 65110063986-76. Below we summarise our high-level response to the consultation, which is followed by answers to the individual questions raised.

Executive summary
AFME recognises FATF's objective of strengthening payment transparency and improving the effectiveness of AML/CFT/CPF measures across cross-border payments and value transfers.

AFME supports the Guidance's efforts to promote a risk-based, proportionate, technology-neutral and outcome-focused framework, enabling consistent implementation of R.16 while recognising the operational diversity of payment systems, payment market infrastructures (PMIs), business models and emerging payment solutions. AFME also supports the continued use of structured data and interoperable approaches that can enhance transparency, consistency and straight-through processing across payment chains.

AFME welcomes FATF's emphasis on a risk-based approach throughout the Guidance and the recognition that implementation approaches may need to reflect differences in payment infrastructures, business models and levels of market maturity. AFME also supports the principle that responsibilities should be allocated to the financial institution best placed to obtain, maintain or validate the relevant information.

While AFME broadly supports the objectives of the Guidance, AFME recommends targeted clarifications in a number of areas to reduce the risk of divergent supervisory interpretations and unintended operational consequences.

In particular, AFME recommends that FATF:

- Preserve the optional nature of the de minimis threshold established under R.16 and avoid creating an expectation that jurisdictions should implement such thresholds where domestic frameworks take a different approach;

- Include additional references to reinforce the distinction between R.16 payment-transparency obligations and Recommendation 10 customer due diligence obligations;

- Clarify that R.16 should not create additional obligations for financial institutions to retrieve or obtain Legal Entity Identifiers (LEIs) beyond information already collected and maintained through existing customer due diligence and customer information processes;
- Recognise 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;
- Further emphasise that the alignment-check measures described in the Guidance represent alternative implementation approaches rather than a hierarchy of controls, allowing financial institutions to apply the approach, or combination of approaches, most appropriate to their business model, risk profile and operational environment.
- Treat alignment mismatches as risk indicators rather than conclusive evidence of fraud or error.
- Ensure that implementation of alignment checks remains consistent with applicable data protection frameworks, including an appropriate legal basis for the collection, transmission, retention and onward sharing of payment information across multi-jurisdictional payment chains.

<u>AFME's response to consultation questions</u>

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

AFME considers that the scope and terminology in Chapter 3 are broadly clear. However, further clarification would support consistent implementation across jurisdictions, payment models and payment-chain participants, particularly where requirements depend on infrastructure readiness, data availability or the role performed by a specific participant in the payment chain.

Scope – Timeline implementation
AFME notes that the implementation timeline described in the Guidance appears broader than that reflected in the Interpretive Note to R.16, which refers to implementation of most requirements by the end of 2030. We request FATF to clarify the relationship between these provisions to avoid divergent interpretations. FATF could further clarify that the 2030 implementation objective should be applied in a manner that recognises jurisdiction-specific implementation pathways and sequencing, particularly where significant infrastructure development, industry coordination or regulatory change is required.

During the transition period, supervisory and enforcement approaches should remain proportionate to the implementation stage, the availability of the necessary legal and regulatory framework, infrastructure readiness and demonstrated good-faith implementation efforts. Jurisdictions should avoid sanctioning institutions for dependencies that cannot reasonably be resolved before the relevant regulatory, scheme or infrastructure changes are in place.

Scope – Fraud
AFME supports further clarification of the relationship between fraud prevention and AML/CFT objectives under R.16. While fraud is now explicitly included within the objectives of R.16, fraud prevention and AML/CFT monitoring may be subject to different legal, governance and data

protection considerations. AFME recommends that FATF clarify how these objectives interact in practice and provide illustrative examples of fraud-related scenarios relevant to R.16 to support consistent implementation across jurisdictions.

AFME also recommends that FATF clarify the distinction between fraud and misdirected payments, and use the latter term where intent has not been established. While fraud may result in a payment being misdirected, misdirection may also arise from non-malicious customer error, inaccurate beneficiary information or operational issues. A clear distinction between these concepts would help ensure that financial institutions apply proportionate controls and do not treat every instance of misdirection as a fraud event.

Legal Entity Identifiers
FATF notes that '*The ordering FI must include the identifier where it reasonably ascertains that one exists, even if it has not been previously obtained by the ordering FI...*' and 'reasonably ascertains one exists, even if it has not been previously obtained.'

AFME supports the clarification regarding the use of LEIs, BICs and other legal-person identifiers, however FATF guidance should avoid creating an expectation that 'reasonably ascertains' means creating a requirement for institutions to proactively identify, retrieve or validate LEIs beyond existing CDD and customer-information processes. This creates the impression that the guidance is going beyond the mandate of the standard and the interpretive note. The timeliness and accuracy of such identifiers should continue to be governed through established CDD and ongoing customer-information maintenance frameworks.

LEIs are valuable identifiers that can support transparency, fraud prevention and AML/CFT controls. However, LEIs generally identify legal entities rather than individual branches and, in some cases, the same LEI may be used across branches operating in multiple jurisdictions. FATF may therefore wish to note as an example in the guidance that in some instances LEIs should be viewed as complementary identifiers and may not, on their own, provide sufficient granularity in all circumstances where branch-level information is relevant.

Terminology - Value transfer definition distinguished from traditional payments
AFME notes that 'payments or value transfers' are defined in the FATF Standards. AFME notes FATF's efforts to harmonise the treatment of payments and value transfers under R.16. To support consistent implementation across jurisdictions, operational scenarios and business models, within the guidance document, FATF could consider providing additional examples illustrating the application of the concept of 'value transfers' in practice.

This would help as in practice, financial institutions and payment system regulators do not always distinguish between these concepts, particularly in account funding, securities-related transfers, wallet funding arrangements and other mechanisms involving scenarios where the movement of value between parties may be operationally indistinguishable from a payment transaction.

Scope - Payment transparency requirements distinct from CDD
AFME welcomes the clarification throughout the Guidance that R.16 payment transparency obligations are distinct from customer due diligence and customer identification requirements under FATF Recommendation 10. Despite the distinction already reflected in some sections of the guidance, several provisions referring to accuracy checks or verification could still be interpreted inconsistently in implementation. FATF could therefore place further emphasis in particular sections that appear ambiguous to support consistent supervisory and industry interpretation. This would ensure provisions are not interpreted as introducing broader customer due diligence obligations beyond those already required under Recommendation 10. As an example, paragraph 77 under section 4.4 which refers to 'Accuracy checks of originator information, and the verification of the beneficiary's identity could trigger the detection of suspicious transactions'.

AFME welcomes FATF's recognition that a variety of methods may be used to support information verification. However, FATF could clarify the role of analytical, inferred or AI-assisted techniques in this context. Financial institutions rely on the accuracy and reliability of information transmitted through the payment chain for sanctions screening, transaction monitoring and other financial crime controls. AFME therefore suggests clarifying that such techniques should complement, rather than replace, information obtained from reliable sources, to mitigate the risk of inaccurate information being transmitted through the payment chain.

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).

As a general overarching comment, it is important to recognise that some implementation requirements depend on changes to PMIs, messaging standards, scheme rules, card-scheme systems and processes, or cross-industry data models, and that financial institutions may not be able to implement such changes unilaterally. We request that FATF work with the national competent authorities for allowing proportionate transition arrangements that reflect infrastructure readiness, industry coordination dependencies and the need to avoid disruption to payment processing.

Domestic payment infrastructures used for cross-border

Yes, AFME considers that the principles of payment-chain definition and their application are broadly clear. AFME welcomes FATF's recognition that domestic payment infrastructures may increasingly be used to process parts of cross-border payment chains.

As additional guidance, FATF could provide additional practical examples and implementation guidance to support PMIs in ensuring that the cross-border nature of a payment remains visible throughout processing and is not obscured when routed through domestic infrastructures.
More generally, obligations should remain clearly allocated and should not require participants to assume responsibilities for information that they do not originate, maintain, control, or have visibility of within the payment chain. This principle is particularly important in complex payment chains involving multiple service providers, net settlement arrangements, bulk or batch processing models, and PMIs.

Debit and pull-payment models

AFME recommends that FATF provide additional guidance on the application of R.16 to debit and pull payment arrangements used in wholesale clearing and custody, including CCP variation margin collection, custodian/tri-party collateral movements and correspondent banking arrangements involving direct debit mandates. In these models, the financial institution debiting the payer's account may not always have practical access to the payee information needed to populate R.16 data. Responsibilities should therefore be assigned based on the role performed in the payment chain, the scheme structure of the relevant payment method, and the entity with practical access to the required data.

The Guidance should avoid a one-size-fits-all assumption. AFME further supports the principle that the payer's financial institution is always the operational starting point for R.16 data obligations in debit or pull-payment models.

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).

AFME believes that PMI data-storage or token-reference models may support compliance with Recommendation 16 when enabling participating FIs to have timely, reliable access to accurate beneficiary details, including the beneficiary financial institutions and underlying account relationship (s). This can promote greater transparency and improve the effectiveness of sanctions screening, transaction monitoring, investigations, suspicious transaction reporting, and alignment-check processes by reducing reliance on data provided by the originator and beneficiary information. Such models may improve payment transparency by creating a consistent source of beneficiary information across participating institutions, while reducing the need for each payment message to carry all underlying data elements where these are securely retained and accessible through the PMI. However, the Guidance should avoid assuming that tokenisation alone is sufficient; the compliance outcome depends on the availability, quality, usability and accessibility of the underlying data.

AFME recommends that FATF clarify the conditions under which financial institutions may rely on PMI-held data, including clear secure and timely access rights, data quality standards, operational resilience, auditability, governance arrangements, liability allocation and the ability to retrieve the underlying information promptly for screening, monitoring, investigations, suspicious transaction reporting and competent-authority requests.

The Guidance should also recognise that the effectiveness of PMI token or data-storage models may depend on common industry standards for data fields, reference formats, access protocols, privacy and data-retention arrangements. A consistent approach would help avoid fragmentation and ensure that token-reference models support, rather than weaken, end-to-end payment transparency.

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).

De minimis thresholds
AFME notes a level of inconsistency between the interpretative note to R.16 and the draft guidance which creates a lack of clarity. R16 and its interpretative note (INR16) 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 noting paragraphs 8 and 10 of INR16 states '*Countries may also adopt a de minimis threshold'.*
The accompanying Guidance appears to go beyond this in paragraph 176. AFME therefore encourages FATF to avoid creating the impression that implementation of a de minimis threshold is expected, where the Standard intentionally leaves this decision to national discretion.

Targeted financial sanctions constitute one of the objectives of R.16 as recognised in paragraph 16(c) of the Guidance. From a sanctions perspective, jurisdictions considering the introduction of a de minimis threshold should take into account that targeted financial sanctions apply irrespective of the amount of a payment or value transfer. Where key payment information is not required to accompany lower-value transactions, this may reduce the information available to support sanctions screening and the identification of designated persons or entities. AFME therefore supports preserving the flexibility provided by INR.16 for jurisdictions to determine whether and how de minimis thresholds are applied, taking into account their own AML/CFT/CPF, sanctions, financial inclusion and broader financial crime risk considerations.

Alternative information
AFME recognises the financial inclusion objectives underpinning the use of alternative information and fallback options where standard payment transparency information is unavailable.

FATF should clarify that 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. Alternative data elements should only be used where there is no choice and should remain sufficiently standardised, structured and interoperable to support effective downstream controls. Financial institutions should remain permitted to request the relevant standard data where they consider that the alternative information provided is insufficient or unsuitable for the performance of those controls. This would avoid creating unnecessary operational complexity or reducing the effectiveness of payment transparency measures.

Name truncation
AFME supports FATF's objective of ensuring that information accompanying a payment is sufficiently detailed to identify the originator and beneficiary throughout the payment chain. AFME welcomes the alignment of R.16 with Regulation (EU) 2023/1113 regarding the requirement to transmit the debtor's and creditor's full name. At the same time, the Guidance recognises that technical constraints may arise in very limited circumstances, including name truncation in legacy infrastructure environments. AFME recommends 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, pre-alignment checks and payment-transparency controls.

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)

Interplay between CDD and payment verification
In line with AFME's response to consultation question 1 regarding the distinction between due diligence obligations, in practice to verify the originator's address, financial institutions generally rely on information obtained and verified during customer onboarding and ongoing customer due diligence processes, using risk-based methods and reliable independent sources in accordance with applicable legal and regulatory requirements, rather than conducting a separate verification exercise for each payment transaction.

Consistent with footnote 49, FATF may also wish to emphasise that the Guidance does not prescribe a specific verification methodology. Different verification mechanisms may be appropriate depending on a range of factors including the product, business model, customer relationship, payment model and risk context.

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

Although there are notable practical limitations of address verification in some jurisdictions, AFME considers that the examples within the guidance are sufficient to support implementation in lower capacity contexts. In particular, the Guidance appropriately recognises that standardised address information and traditional verification methods may not be available in all jurisdictions and provides useful flexibility regarding alternative information and verification approaches. AFME has no further comments in relation to this 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).

AFME considers that the measures set out in the Guidance are generally clear and actionable.

AFME welcomes the measures proposed regarding virtual account numbers. To support consistent implementation, AFME recommend that FATF clarify that responsibility for ensuring that account numbers are not used to disguise the country of the servicing financial institution should rest with the financial institution operating or controlling the underlying master-account structure, as that institution is best placed to possess and maintain the relevant information.

In many cases, other participants in the payment chain may not have visibility that a virtual account structure is being used and therefore may not be able to identify or address any resulting transparency risks.

AFME notes that some jurisdictions are already developing specific mechanisms to improve transparency in virtual-account structures, including centralised repositories.

AFME recommends 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.

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).

AFME does not have any specific comments to provide in response to this 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).

AFME does not have any specific comments to provide in response to this 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).

AFME does not have any specific comments to provide in response to this question.

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

AFME considers that Chapter 8 largely provides sufficient clarity and supports FATF's payment-method-neutral approach and welcomes the Guidance's discussion of instant payments, digital wallets, mobile money and proxy identifiers. Considering that payment methods evolve quickly, the Guidance should continue to remain focused on equivalent transparency outcomes rather than prescribing payment-rail-specific implementation approaches.

Additional clarity would be helpful regarding the application of R.16 in instant-payment environments, including the treatment of proxy identifiers, the resolution of required information and the balance between effective controls and payment friction.

The Guidance should avoid implying that R.16 requires a specific real-time screening, pre-validation or operational model where this is not otherwise prescribed by local law, regulation or scheme rules.

Effective Travel Rule compliance depends on the ability of ordering and beneficiary virtual asset service providers (VASPs) to identify, authenticate and securely exchange the required information. In practice, the use of fragmented or non-interoperable Travel Rule solutions may prevent VASPs from transmitting or receiving the required information, performing pre-validation checks, or confirming successful delivery of Travel Rule data. This may undermine the payment-transparency objectives of the Travel Rule, despite reasonable compliance efforts by the parties involved. AFME therefore encourages FATF to recognise interoperability as a key component of effective Travel Rule implementation and to promote interoperability between Travel Rule solutions in a technologically neutral manner. FATF should also clarify the responsibilities of an ordering VASP where a beneficiary VASP is not reachable through its Travel Rule solution and whether a transfer may proceed where the required information cannot be transmitted prior to execution due to interoperability constraints.

AFME notes that, unlike many traditional payment arrangements, a beneficiary VASP may have no technical ability to prevent a third party from initiating an on-chain transfer to a published or previously allocated wallet address. By the time the transaction is detected, it may already have been confirmed on the blockchain and cannot ordinarily be suspended or rejected at protocol level.

Additional clarification would therefore be helpful regarding the responsibilities of a beneficiary VASP where crypto-assets are received without the required Travel Rule information, particularly where no originating VASP can be identified. FATF should clarify the reasonable steps expected of a beneficiary VASP to obtain the missing information, the measures that should apply while information is outstanding, and the factors that should be considered when determining whether assets may be credited, restricted, returned or otherwise handled. Any guidance should recognise the technical limitations of blockchain-based transfers and support a proportionate, risk-based approach.

12)Is there any additional guidance that would address potential challenges in implementing R.16 with respect to data protection and privacy? (Chapter 9).
AFME welcomes the data protection considerations included in Chapter 9. Certain measures discussed in the Guidance, including holistic ongoing monitoring frameworks, profiling techniques and AI-assisted controls, may be subject to Data Protection Impact Assessments (DPIAs) and related governance requirements under applicable data protection frameworks. To support consistent implementation, AFME recommends that FATF clarify that implementation of R.16 should remain consistent with applicable data protection frameworks, including the legal bases available for collecting, transmitting, retaining and sharing personal data for AML/CFT, sanctions and payment-transparency purposes.

AFME notes that paragraph 240 appears to frame relevant processing activities primarily by reference to public-interest objectives. While AML/CFT objectives serve an important public interest, obliged entities typically process personal data pursuant to applicable legal obligations under national or regional AML/CFT frameworks. FATF could therefore clarify that implementation of R.16 should remain consistent with the legal bases available under applicable data protection frameworks, including processing required to comply with AML/CFT legal obligations.

AFME supports the data minimisation principle reflected in Chapter 9. To support consistent implementation, FATF could further clarify the categories of personal data that are necessary to achieve R.16 objectives and confirm that financial institutions should not be expected to collect or process additional personal data beyond what is necessary for AML/CFT, sanctions and related payment transparency purposes.

We request FATF provide additional clarity regarding responsibility for transparency and information obligations where personal data is exchanged among multiple financial institutions, PMIs and other payment-chain participants. In particular, the Guidance could clarify the application of indirect collection exemptions where information is obtained from another payment-chain participant rather than directly from the data subject.

AFME also recommends that FATF acknowledges the cross-border data-sharing challenges that may arise where R.16 information is transmitted through multi-jurisdictional payment chains

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).

AFME welcomes FATF's decision to provide multiple alignment-check options and generally considers the available approaches to be sufficiently clear for implementation. However, certain passages, including references to post-validation checks as a 'fallback' measure and examples describing pre-validation as the primary approach where available, may be interpreted as implying a preference for particular implementation models. Given the diversity of payment systems, business models and fraud risks, it is important that the Guidance continues to support a risk-based, proportionate and outcome-focused approach.

AFME notes that the proposed alignment check framework may require further adaptation to reflect the specific characteristics of virtual asset transfer. Unlike traditional payment arrangements, an on-chain transaction typically contains a wallet address but not the beneficiary's verified identity. A wallet address is a technical identifier and does not itself evidence the identity of the person controlling it particularly where wallets are pooled, rotated or managed through omnibus arrangements.

AFME recommends that the guidance confirm that a VASP-to-VASP alignment check is intended to verify that:

- The destination wallet address is controlled or serviced by the beneficiary VASP
- The address is associated with the intended beneficiary
- The beneficiary information transmitted is sufficiently consistent with the beneficiary VASP's own records
- The beneficiary VASP can receive the required Travel Rule information through an appropriate secure channel

AFME would encourage FATF to clarify that the three options are not intended to establish a hierarchy between pre-validation, post-validation and ongoing monitoring and that financial institutions may select the approach, or combination of approaches, most appropriate to their business model, risk profile and operational environment. Virtual asset transfers warrant a different emphasis, and the instantaneous and irreversible settlement is a risk factor that often makes pre-validation the more effective choice for virtual assets on a risk-based approach. FATF could also provide further practical examples illustrating how the different approaches may be applied across a range of payment types, legal frameworks and levels of market maturity, including where broader fraud prevention programmes, customer education and preventive, detective and responsive controls may achieve equivalent outcomes. AFME recommends that FATF clarify that alignment checks do not alter the fundamental principle that the originator (debtor) remains responsible, first and foremost, for providing accurate beneficiary (creditor) details and authorizing the payment. Alignment checks should be viewed as an additional fraud mitigation tool rather than a substitute for the originator's responsibility and should not be viewed as transferring responsibility for payment initiation accuracy from the originator to the creditor agent.

The Guidance should avoid introducing unnecessary friction into cross-border payment processes, particularly where payment participants operate across multiple jurisdictions and infrastructures.

AFME recommends that FATF clarify alignment-check obligations should not be interpreted as requiring beneficiary financial institutions to perform mandatory real-time or pre-credit name/account matching in all cases. In some jurisdictions and payment systems, including high-volume payment systems and systems subject to settlement-finality rules, payments may be processed based on account identifiers and governed by legal or scheme frameworks that do not contemplate beneficiary-name matching as a condition for acceptance or crediting.

Holistic ongoing monitoring should remain a risk-based monitoring framework that may include real-time, near-real-time, or post-event controls depending on the payment rail, legal framework, customer risk, corridor risk, and operational feasibility.

Where a mismatch or potential misalignment is identified, the result should be treated as a risk indicator rather than a conclusive determination of fraud or error. Follow-up actions should be proportionate and consistent with local law, scheme rules, payment finality requirements, and the financial institution's broader fraud, AML/CFT, and misdirected-payment controls.

We would welcome the opportunity to discuss any point made in this paper with FATF colleagues if helpful and we look forward to supporting you in your work.

AFME Contacts

Hanna Sowemimo
Hanna.sowemimo@afme.eu
Associate Director
+44 7825081684

Ria Mehta
Ria.mehta@afme.eu
Associate
+44 7901324086