

May 2, 2024

To: Ms Violaine Clerc
Executive Secretary
Financial Action Task Force ("FATF")

Via electronic submission to: FATF.Publicconsultation@fatf-gafi.org

Dear Ms. Clerc,

Subject: Response to FATF Public Consultation on Draft R.16 Amendments

The Payments Market Practice Group ("PMPG") is an independent body of payments subject matter experts from Asia Pacific, EMEA and the Americas, forming a truly global forum to drive better market practices.

As a group of payments practitioners, the PMPG therefore greatly appreciates the opportunity to contribute to the public consultation on the draft amendments to FATF Recommendation 16 (R.16) and welcomes the opportunity to share our global expertise and observations, aiming to assist the FATF in achieving its objectives.

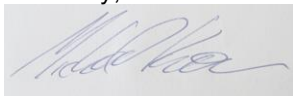
We commend FATF's commitment to ensuring that the principle of "same activity, same risk, same rules" is upheld throughout the update of R.16, contributing to the G20 Cross-Border Payments objectives. The PMPG is concerned that applying a single solution may not adequately address the risks and could result in unintended negative consequences for corporates and consumers, such as increased costs and processing times. We value the comprehensive approach and propose including customer due diligence measures (KYC processes), enhanced regulatory supervision for non-bank Payment Service Provider (PSPs), and clarification on the roles and responsibilities of each PSP and Payment Market Infrastructure (PMI) in the payment chain. We emphasize the importance of involving all stakeholders in the payment ecosystem in the dialogue and scope of R.16 to ensure effective risk mitigation.

We also highlight the importance of distributing the responsibility for addressing financial crime risks through payment transparency across all stakeholders. PMPG is committed to collaborating further to clarify any outstanding questions and to find the best available options for addressing the objectives, taking into account the maturity of markets globally.

Attached to this letter is our detailed response to the consultation, with our answers embedded in the FATF document in **blue** boxes for clarity. Our recommendations/additions to the glossary are highlighted in **purple**.

Thank you for considering our input - we look forward to continued engagement and collaboration with FATF on this critical matter.

Sincerely,



Michael Knorr
Co-Chair of the Payments Market Practice Group

This Explanatory Memorandum is intended to facilitate consultation on the proposed revisions to FATF Recommendation 16, its Interpretive Note (R.16/INR.16) and the related Glossary of specific terms, and should be read alongside the attached redline document, which sets out the text of the revisions. This note explains the policy intent behind each of the proposed changes, the considerations, which have shaped the approach proposed, and asks specific questions to which the FATF invites responses. The FATF invites input on the specific questions set out in this note, as well as on other issues covered by the proposed amendments to R.16/INR.16 and the related Glossary of specific terms as reflected in the redline text.

The FATF recognises that due to the technical nature of this subject, a full consultation will require an ongoing dialogue with the relevant bodies and experts in both public and private sectors. This written consultation is the first step in a wider consultation process, which will also include further discussion and engagement, as needed, informed by the responses to this initial consultation.

Following finalisation of the revisions, the FATF will develop a Guidance paper on payment transparency in order to facilitate consistent implementation of FATF Standards between jurisdictions. It will be helpful if responses also highlight any issues, that would require further clarification through subsequent Guidance paper, or which raise particular challenges for implementation.

Objective of the proposed revisions to R.16/INR.16

The FATF has worked on updating R.16/INR.16 to adapt them to the changes in payment business models and messaging standards. There is a need for R.16/INR.16 to be updated to ensure that the FATF Standards remain technology-neutral and follow the principle of 'same activity, same risk, same rules'. This project is also a part of the G20 Priority Action Plan to progress work on making cross-border payments faster, cheaper, more transparent and more inclusive, while maintaining their safety and security. Revisions include clarifying the roles and responsibilities of different players involved in the payment chain and improving the content and quality of basic originator and beneficiary information contained in the payment messages. This should help achieve greater transparency and more efficient and effective compliance processes by financial institutions.

Proposed revisions to R.16/INR.16

The proposed revisions to R.16/INR.16 and the related Glossary of specific terms are attached to this Explanatory Memorandum, and the policy intent of the key proposals for revisions is explained in detail below.

a. Terminology changes

Potential amendments were sought to modify the terminology used in R.16/INR.16 to align the text with the terms that are commonly used in the payment messages such as ISO 20022 (e.g., 'debtor', 'creditor'). The FATF also considered that several key terms that have been used in R.16/INR.16 (e.g., 'originator' and 'beneficiary') are well understood by the stakeholders. Therefore, it is proposed to retain such key terms and add footnotes (*footnotes 46 and 49 of INR.16*) to cross-reference the terms used in ISO 20022 for alignment. The title of R.16/INR.16 is also proposed to change from 'Wire transfers' to 'Payment transparency', to be platform-neutral and better align with the obligations set out in the Standard.

b. Retaining the existing exemption for purchase of goods and services, subject to additional transparency requirements (paragraph 4 (a) of INR.16)

Currently, transactions carried out using a credit, debit, or prepaid card for the purchase of goods or services are exempt from R.16, so long as the card number accompanies all transfers flowing from the transaction. This exemption does not apply to person-to-person transfers carried out using a credit, debit, or prepaid card.

Card payments may present lower illicit finance risks than some other forms of payment, such as wire transfers. Card payments ecosystems are closed systems, in which participating cardholders and merchants are customers of financial institutions, which in turn are contractually obligated by the card network to adhere to certain AML/CFT and sanctions compliance measures. This was the basis for the current exemption.

Nevertheless, cards are not free from illicit finance risks. FATF delegations have observed case studies and typologies that show several ways in which various types of payment cards can be, and are, used for money laundering and terrorist financing. These include for example:

- The use of credit and debit cards and fake merchants to disguise purchases of illicit goods as legitimate purchases.
- The use of shell companies to open offshore bank accounts with merchant acquiring banks to accept credit/debit card charges for illicit goods purchased.
- The use of stolen credit card numbers from black market websites to encode that information onto blank cards, and use of such cards to purchase gift cards or other items that can be quickly sold for cash.
- Exploitation of front companies by money laundering syndicates. These companies obtained funds with unknown sources from another jurisdiction, after which they converted the funds by purchasing a large quantity of stored value cards. These cards were subsequently used to purchase gift cards which were then extended to other jurisdictions.
- Use of a foreign issued debit card in tax evasion schemes to receive payout to the company's foreign bank account. A foreign issued debit card is used for ATM cash withdrawals and immediately deposited in domestic bank accounts.
- Loading of foreign prepaid cards with cash from different locations in one country or through online transactions, and subsequent withdrawal of cash in another country with small time difference between deposits and withdrawals, raising potential TF and sanctions evasion concerns.

In addition to the illicit finance risks, changes in the market have blurred the distinction between purchases of goods or services and person-to-person transfers, widening the payment card exemption far beyond its original scope. For example, cards can be used to initiate Money or Value Transfer Services (MVTs) payments, purchase cash substitutes online, withdraw cash at ATMs, and purchase goods and services on online marketplaces from other individuals, without any checks on whether these transactions are indeed for the sale of goods or services. Another reason to revisit the card exemption is to ensure that it is not misused for purposes other than the original objectives and to maintain the principle of "same business, same risks and same regulation" to the extent appropriate, by applying a consistent approach, irrespective of differences in the means of payment used.

The FATF is considering two options for amendments to address the issues above and to ensure transparency and adequate AML/CFT controls. Recognising that changes to this requirement potentially carry significant costs and may require some time to implement in the context of existing payment systems, the FATF invites industry views on the merits, the costs, and the implementation issues associated with each option.

Option 1 would clarify that only transfers that flow from a transaction carried out using a card for the purchase of goods or services from '**merchants**' (a newly defined term in the Glossary) are exempt from the requirements under R.16. This option would also require that the card number and '**the name and location of the issuing and acquiring financial institutions**' accompany the transfer. The inclusion of issuer and acquirer information would unambiguously identify the specific financial institutions that have customer relationships with the cardholder and merchant in a given transaction and would lead to better

transparency for all financial institutions involved in the payment chain, appropriate law enforcement and FIU authorities, as necessary. This proposed new requirement aligns with the principle that is considered throughout revisions to R.16: to enhance the transparency about the financial institution that holds the customer's account and is the origin of the funds. This proposal is expected to provide equally robust AML/CFT controls as the present R.16, and it entails lower costs and raises fewer data privacy and protection (DPP) concerns than applying the same information requirements to the parties involved in card payments, such as the ones prescribed under paragraph 7 of INR.16. This option would enable financial institutions, law enforcement and FIU authorities to obtain information on the originator and beneficiary by ensuring adequate transparency of the name and location of the issuing and acquiring financial institutions, which could then be approached where appropriate.

Option 2 builds upon Option 1 and further removes '**withdrawal or purchase of cash or a cash equivalent**' from the scope of the R.16 exemption (in addition to the existing exclusion of person-to-person payments). This is intended to address the lack of transparency in foreign ATM withdrawals and purchases of cash or cash equivalents, which are not characterised as the purchase of goods or services. However, this would not apply to situations in which cash is being withdrawn by a person from the financial institution at which he or she is holding the account.

Option 2 proposes different approaches for the application of the new requirements on withdrawal or purchase of cash or a cash equivalent in the domestic and cross-border contexts. While the requirements are proposed to be applied for cross-border withdrawal or purchase of cash or a cash equivalent without any monetary threshold, for domestic withdrawal or purchase of cash or a cash equivalent, these requirements would apply only for transactions with value above 1000 EUR/USD. This distinction for cross-border and domestic transactions is to ensure a proportionate and risk-based approach with due consideration of other policy objectives, such as financial inclusion.

This measure is intended to enable relevant financial institutions in the payment chain to more effectively detect illicit use of cash withdrawals, including smurfing/structuring activity (multiple withdrawals by the same individual using different cards), fraudulent use of cards, and evasion of targeted financial sanctions. Ensuring that the identifying information is available to the beneficiary financial institution (which is dispensing the cash or cash equivalent) would enable increased transparency, and that information is readily and more rapidly available to relevant investigative authorities.

Questions for consultation on the card exemption

Q.1 - Do you support FATF's proposal above? If so, which option will be better and why? If you do not support FATF's proposal, please explain why. Are there any appropriate alternative proposals to ensure transparency, adequate AML/CFT controls and level playing field while minimising the unintended consequences?

<p>PMPG</p>	<p>The PMPG is fully supportive of efforts to mitigate financial crimes by ensuring existing gaps are effectively addressed, and doing so without the introduction of unintended consequences, including significant implementation cost, higher operating cost/complexity, and disproportionately negative client experience for no/low risk transactions.</p> <p>As noted in FATF's memorandum, the current card exemption is based on the nature of the card payment ecosystem, which is inherently a closed one. This structure remains unchanged, as participating cardholders and merchants are customers of financial institutions, and, as a result, are contractually obligated by the card network to adhere to certain AML/CFT and sanctions compliance measures.</p> <p>Whilst FATF highlighted uses cases in which card payments can be deployed illicitly (money laundering or terrorist financing), these cases are best addressed through the fortification of account opening and KYC processes rather than the introduction of additional data accompanying the payment. In fact, merchants, acquirers, Financial Institutions (FIs) and end users all must be clients of either a regulated financial institution or have a relationship with the card network. This means that card networks serve as the 'integrator', and they hold critical information about the debtor and creditor, often via BIN</p>
-------------	---

	<p>for issuers, Acquirer ID, settlement/authorization reference IDs (networks maintain look-up directories to identify the issuer and acquirer of each transaction). As a result, it would be more prudent to focus on mechanisms for law enforcement agencies to easily access this information from the card network directly vs from financial institutions. We encourage FATF to better clarify roles and responsibilities of parties in this closed ecosystem and to do so by leveraging existing tools available, rather than defining roles and responsibilities that will require significant technology investments for other parties to access the same information.</p> <p>Furthermore, FATF noted concerns with the use of stolen card credentials (physical or virtual). Whilst this is a valid concern, this risk is best mitigated through stronger authentication control at ATMs, third-party wallets, Point of Sale systems, financial institutions' online channels, and eCommerce merchants, rather than requiring additional data to be shared in the payment message, which will not materially address risk.</p> <p>We believe that credit card and debit card transactions, whether they are commerce, eCommerce, ATM cash withdrawals, funds transfer (P2P) or funds disbursement (B2C), have strong built-in controls and greater transparency than cash transactions or other non-card transactions. However, pre-paid cards (reloadable and non-reloadable), which by their nature do not have transparency about the end user, can more readily be deployed for Money Laundering or Terrorist financing. Nevertheless, we believe that the requirement for additional payment data will not necessarily address this gap. Instead, we encourage FATF to work with pre-paid card providers to develop controls associated with the sale, transaction limits, distribution and fund disbursement of pre-paid cards vs creating payment data requirements across credit, debit and prepaid more broadly.</p> <p>The PMPG recommends that FATF adopts a payment-agnostic stance and extends current card exemptions to instant and faster payment and other closed-loop payment systems used for the purchase of goods and services. Any payment used in this scenario should be treated the same (e.g., European Payment Initiative, FedNow, RTP, NPP, PIX, TIPS).</p> <ul style="list-style-type: none"> • Option 1: The PMPG recommends that FATF clarify the roles of individual parties in the closed card ecosystem system (existing and emerging, such as wallets) and assess the need for stronger merchant/acquirer account management processes, as well the ability for law enforcement agencies to obtain more quickly the necessarily information from card networks. • Option 2: The PMPG is not supportive of Option 2. This option introduces data requirements akin to wire payments, and, in doing so, discount the fact that ATM credit or debit withdrawals access funds in the client's own account, where there is no transfer of funds, and where account ownership is clear regardless of whether these transactions happen via domestic or international ATMs. Furthermore, the PMPG believes that this option does not provide any additional transparency regarding the cash movement post-withdrawal - it is vague about the definition of 'cash-equivalent' and it could impact access to cash for international clients and would require a substantial overhaul to the ATM infrastructure across the world, with limited incremental benefits.
--	--

Q.2- *Are there any important aspects that the FATF needs to consider in finalising the revisions to R.16 and working on FATF Guidance on payment transparency in order to facilitate consistent implementation of FATF Standards between jurisdictions, based on considerations such as feasibility of the proposals, timeline of implementation and mitigation of unintended consequences such as disproportionate impact on cost, financial inclusion, and humanitarian considerations?*

PMPG	<p>Several important considerations for card exemptions include:</p> <ul style="list-style-type: none"> • The cost required in both options, which seek to align the card ecosystem to 'wire-like' payments, will be significant and, ultimately, will negatively impact merchants
------	---

	<p>and clients. Card payments already have greater transparency about ‘actors’ in the payment chain, and FATF is encouraged to amend the Recommendation to better define roles and responsibilities, as well as focus on access existing information held by key parties.</p> <ul style="list-style-type: none"> • The payment industry is evolving rapidly, with new solutions for commerce, including tokens, wallets, commerce marketplaces, QR codes for instant payments, or cryptocurrency. This proposal is silent on requirements for these transactions. That is, by focusing primarily on card transactions, which already have more transaction data than the emerging alternatives, it could shift activity from card transactions, thus creating an uncompetitive landscape and shifting higher-risk transactions to the emerging alternatives. • Most card networks do not currently use the ISO 20022 scheme. Whilst they may seek to adopt ISO 20022 in the future for various strategic reasons, this change should not be driven by FATF R.16. It does not inherently introduce greater safeguards or transparency compared to the currently used schemes. • Prepaid cards are heavily used in markets with high underbanked populations or for government fund disbursement to low income/vulnerable populations. FATF requirements for card payments must consider the financial viability of these services, and the negative impact it might introduce to certain client segments, if applied broadly. It is recommended that R.16 focuses on ‘source of the risk’ by reviewing requirements associated with the KYC processes of these government programs.
--	---

Q.3- *Which data fields in the payment message could be used to enable financial institutions to transmit the information on ‘the name and location of the issuing and acquiring financial institutions’ in a payment chain? If appropriate data fields or messaging systems are not currently available, how could they be developed and in what timeframe?*

PMPG	See Q.1 response. Information about name and location of issuing FIs are already part of the card infrastructure, and this information should be accessed through the card networks’ existing capabilities/database. instead of requiring this information to be shared in the transaction messages themselves. PMPG highly recommends FATF consults with the main card networks about available databases and timely access to them.
------	---

Application of the exemption to different card types

While some types of cards could demonstrate unique risks because of their features and characteristics (e.g. anonymity, lack of adequate customer due diligence measures and absence of ongoing relationship of the card holder with the financial institutions), typologies also demonstrate that much of the risk for cards applies equally across credit, debit, and prepaid products (such as risk of skimming, fraudulent transactions, transferability of cards to third parties and across different locations and across national borders). In addition, credit, debit, and prepaid card transactions are processed on the same payment rails by card networks, and it may be more difficult to apply certain measures to specific card types than it is to apply measures equally across all card types. For these reasons, the proposed options for the amendment of the card exemption apply equally to credit, debit, and prepaid cards. The FATF has also considered that it is not appropriate to extend the card exemption to other payment means (e.g., instant payments), which can also be widely used for the purchase of goods or services, due to different nature of the associated risks with other payment means. The FATF will prepare a more detailed Guidance document on payment transparency following adoption of amendments to R.16, which could include more granular guidance on potentially different risk profile and mitigation measures between credit, debit and prepaid cards, and the analysis of other payment means, and applicable risk mitigation measures as needed.

Questions for consultation

Q.4 - Do you support the FATF's proposal to apply the amended card exemption equally to credit, debit, and prepaid cards? If not, why? Are there any appropriate alternative proposals? In terms of the potential differences in AML/CFT risk profiles and mitigation measures in different types of cards such as credit, debit, and prepaid cards, are there any aspects that FATF should pay due attention in finalising revisions to R.16 and in developing the future FATF Guidance on R.16? If so, what are they?

PMPG	<p>Noted above.</p> <p>Pre-paid cards (reloadable and non-reloadable), which by their nature are closer to cash transactions as they do not have end-user transparency and, as such, can more readily be deployed for Money Laundering or Terrorist financing. Nevertheless, we believe that the requirement for additional payment data will not necessarily address this gap. Instead, we encourage FATF to work with pre-paid card providers to develop controls associated with the sale, transaction limits, distribution and fund disbursement of pre-paid cards vs creating payment data requirements across credit, debit and prepaid more broadly.</p> <p>The usage of pre-paid cards for government fund disbursement to vulnerable populations do have better transparency than pre-paid cards used in other use cases, since both the party disbursing funds (government) and party receiving funds are known, funds are limited, and usage of funds is often restricted to essential necessities (via recipient attestation). Any gaps to this use case are best addressed through stronger government application oversight, rather than additional information in the payment message.</p>
------	---

Q.5- Considering that the current exemption extends to credit, debit and pre-paid cards, are there any other similar means of payment that should be included in the card exemption for the purchase of goods and services? What are examples of those means of payment, and why should they be included in the exemption?

PMPG	<p>The PMPG recommends that FATF adopts a payment-agnostic stance and extends current card exemptions to instant and faster payment and other closed-loop payment systems used for the purchase of goods and services. Any payment used in this scenario should be treated the same (e.g., European Payment Initiative, FedNow, RTP, NPP, PIX, TIPS).</p>
------	---

Scope of “withdrawal or purchase of cash or a cash equivalent”

Under Option 2, **‘withdrawal or purchase of cash or a cash equivalent’** is proposed to be excluded from the R.16 exemption. The application to cash equivalents is intended to avoid creating loopholes, which would enable circumvention of the requirements applied to cash withdrawals, by using other instruments with a similar risk profile. Further clarity would be needed on what should be considered a ‘cash equivalent’¹. For the purposes of R.16, the term ‘cash equivalent’ could include examples such as purchase of virtual assets and digital currencies, tokens of certain kinds (e.g., casinos and online gambling), etc.

Questions for consultation

Q.6 - Should R.16 apply to cash withdrawals and purchase of cash or a cash equivalent? If so, should it apply to withdrawals using credit, debit, and pre-paid cards in the same way, or

¹ In the context of R.16 “cash equivalent” is used in a different sense to its accounting definition of specific asset classes (e.g., treasury bills, commercial paper, other liquid assets, or commodity assets).

be differentiated according to card type? Should it apply only to withdrawals above a threshold and if so, what is the appropriate threshold?

PMPG	See response to Q.1
------	---------------------

Q.6bis Do you support the FATF's proposed treatment of domestic cash withdrawal? Are there situations in which exemptions should apply (other than domestic withdrawals by a beneficiary from ATMs of financial institution holding its account, in which case R. 16 has no applicability)? Are there any important aspects that FATF needs to consider in terms of implementation of applying R.16 to withdrawal or purchase of cash or a cash equivalent?

PMPG	ATM cash withdrawals, both domestic and international, use clients' own credentials and provide access to clients' own funds. As such, PMPG is unclear as to how any of the additional requirements prescribed by FATF's R.16 Recommendation for cash withdrawals will address the risks noted in the Consultation paper. In fact, applying more requirements for ATM cash withdrawals will not only have significant implementation cost and result in limited benefits, but it will also shift away resources from being able to focus on higher-impact strategies.
------	---

Q.7 - What should be included in the scope of 'cash equivalent'? What aspects regarding the scope of 'cash equivalent' should be further clarified? Should such scope be defined in the standards or clarified in the future FATF Guidance?

PMPG	The term "cash equivalent" should be defined more clearly in light of emerging usage of various value-store alternatives, such as gift cards, crypto-currency and fractional ownership tokens (e.g., real estate). For reference, the U.S. Securities and Exchange Commission (SEC), defines cash equivalents as "highly liquid investments that are readily convertible to known amounts of cash and are subject to an insignificant risk of change in value due to interest rate, quoted price, or penalty on withdrawal."
------	--

c. Improving the content and quality of basic originator and beneficiary information in payment messages (paragraph 7 of INR.16)

Standardised information and enhanced data quality would improve the reliable identification of the originator and beneficiary and increase efficiency, by facilitating automated processing and by reducing the number of false positives in sanctions screening. This would also be useful for the purposes of detecting suspicious transactions, and for investigations. Paragraph 6 of the interpretive note introduces a requirement that the information must be structured in accordance with the established standards such as ISO 20022. Paragraph 7 of INR.16 sets out updated requirements for the specific information that should be included in payment messages. The key change proposed to be introduced is that address would become a mandatory element for both originator and beneficiary. In the absence of address, the country and town name should be sufficient to meet these obligations.

FATF is also considering whether there are potential additional benefits from fully aligning the information required on the originator and the beneficiary, such that the same standardised information set would be required on all customers; and whether these potential benefits may be outweighed by potential frictions introduced by transmitting additional, un-verified, beneficiary information. FATF is considering two options in this regard.

Option 1 is close to the existing requirements with full name, account number (in the absence of account number a unique transaction number) and address for both originator and beneficiary as mandatory elements. Where address is not available, country and town name should be sufficient. Optionality is retained for other required information elements. The addition of 'address' as a mandatory information element both for originator and beneficiary should help financial institutions better comply with their preventive measures, including targeted financial sanctions obligations. The additional mandatory elements of 7(d) and 7(e) are added to strengthen the identification of originator and beneficiary. The

optionality in the mandatory information elements for originator who is a natural person as set out in para 7(d) seeks to provide flexibility in implementation, and should help financial institutions better identify the counterparts of the transaction, taking into account the data privacy issues and concerns. Where originator or beneficiary is a legal person, additional information elements are sought both for originator and beneficiary, as set out in para 7 (e). These information elements should help achieve more efficiency and effectiveness in compliance procedures of financial institutions and provide timely access to relevant information by law enforcement.

Option 2 seeks to achieve full alignment in all information elements for originator and beneficiary. This approach seeks to treat both originator and beneficiary on equal footing in terms of information elements. As with Option 1, this option also seeks to achieve flexibility in case of additional mandatory information elements for both originator and beneficiary, whether natural or legal person, as set out in para 7(d) and 7(e). The full alignment of information elements for both originator and beneficiary seeks to create greater degree of symmetry in payment messages, leading to better compliance by financial institutions and timely access to relevant information by law enforcement.

Question for consultation

Q.8 - Would stakeholders support FATF’s approach and view that the proposed amendments will improve the reliable identification of the originator and beneficiary and increase efficiency? Which of the two options set out above for the proposed revisions in paragraph 7 would stakeholders prefer and why? To what degree is the customer identification number, as set out in paragraph 7 (d), useful to identify the customer? Are there any other issues or concerns in this regard? Are there any important aspects where the FATF needs to provide more granular advice in the future FATF Guidance in order to facilitate effective and harmonised implementation of the FATF proposal?

<p>PMPG</p>	<p>The challenges confronting the objectives of the FATF revised Recommendation warrant careful consideration and a collaborative approach.</p> <p>Whilst the PMPG acknowledges the value in requiring the name and address of the originator and beneficiary, implementing the full beneficiary information, as suggested in Option 2, presents practical difficulties. Besides concerns about data privacy, there is uncertainty regarding the accuracy of unvalidated information, potentially leading to flawed screening by banks. It is essential to recognize situations where disclosing personal identifiers might not be feasible due to concerns about misuse.</p> <p>Whilst we concur with the requirements outlined in Option 1, particularly 7a, b and c, we must confront the significant hurdles posed by the requirements of 7d and e.</p> <p>Addressing these challenges, including customer data privacy worries, technical implementation efforts and potential unintended consequences, is crucial to prevent increased complexity, friction, and costs, as well as the potential diversion of payment volumes into alternative channels.</p> <p>The addition of mandatory organization or private ID elements presents challenges that need careful consideration. Experience with adopting ISO 20022 structured data demonstrates the complex process of capturing, storing, and integrating such elements across various applications and systems. It is also important to note that a considerable portion of payment market infrastructures may not transition to ISO 20022 within a reasonable timeframe. Consequently, any supplementary information could be lost along the payment chain. This introduces a new risk for banks, as they may struggle to comply with the travel rule due to data truncation.</p>
-------------	--

	<p>Furthermore, the reluctance of natural persons to provide personal information, coupled with the lack of relevance of certain identifiers in cross-border payments, presents significant hurdles.</p> <p>For legal persons, national identifiers are ineffective in cross-border transactions, and mandating BIC or LEI for all could disproportionately impact smaller businesses, limiting financial inclusion. Moreover, incorporating additional identifiers into compliance screening processes risks increasing mismatches and false positives, complicating payment initiation and hindering the achievement of G20 objectives.</p> <p>PMPG recommends advocating the provision of the LEI as an <u>additional ID</u> as a best practice; incorporating Private ID should be optional, to be used when necessary for unambiguous identification, rather than imposing mandatory requirements.</p>
<p>PMPG recommendation</p>	<p>In light of the aforementioned concerns and challenges, the PMPG recommends a thoughtful approach to the requirements for the identification of the originator and beneficiary. It is imperative to balance the objectives of enhancing transparency and mitigating financial risk with the practical realities faced by market participants.</p> <p>Recommendation as an alternative option for FATF’s consideration:</p> <p>Financial Institutions should uniquely identify all financial institutions and legal persons in a payment in a standardized and internationally-recognized manner.</p> <p>Information accompanying all qualifying payments or value transfers should always contain:</p> <p style="padding-left: 40px;">(a) the full name of the originator and beneficiary or, where the originator and/or beneficiary is a legal person, then the published business identifier code (BIC) (<i>*footnote (1)</i>),</p> <p style="padding-left: 40px;">and</p> <p style="padding-left: 40px;">(b) the account number of the originator and beneficiary where such an account is used to process the transaction. In the absence of an account, a unique transaction reference number should be included, which permits traceability of the transaction,</p> <p style="padding-left: 40px;">and</p> <p style="padding-left: 40px;">(c) the address of the originator and beneficiary, or, in the absence of an address, the country and town name; (<i>*footnote (1)</i>)</p> <p>Where necessary to achieve unambiguous identification, the originating PSP is encouraged to include additional information, such as:</p> <p style="padding-left: 40px;">(d) where the originator is a natural person, the date and place of birth of the originator,</p> <p style="padding-left: 40px;">or</p>

	<p>(e) where the originator is a legal person, the published Business Identifier Code (BIC), or the Legal Entity Identifier (LEI) (**footnote (2)).</p> <p>* footnote (1) - where structured identifiers are used, the internationally-recognized Business Identifier Code (BIC) is a valid alternative to Name and Address, provided that the Name and Address information associated with the Identifier in the directory aligns with the Name and Address that would otherwise be supplied.</p> <p>** footnote (2) “Under ISO 9362, the BIC contains the two-letter ISO country code where the entity is located, enabling country-level sanction screening on the BIC level without retrieving the related reference data. In the case of LEI, any country identification requires retrieval of the reference data. Depending on the technical set-up of the screening process, this could be deemed less efficient”.</p>
--	---

d. Addressing transparency in case of virtual IBANs and other similar account naming conventions (paragraph 7(b), footnote 1 of INR.16)

In some countries, the use of a virtual IBANs may allow customers to use one or multiple IBANs showing country codes which are different from where their account is actually held. This practice can obscure the true location of the customer’s account and prevent the financial institutions and authorities from identifying the true nature of a transaction (as international rather than domestic transfer) and accessing the necessary information efficiently. Footnote 1 (*‘The account number or the associated payment message data should enable the institutions and authorities referred in paragraph 1 to identify the financial institution and the country where the account holder’s funds are located.’*) to paragraph 7(b) seeks to ensure that, in cases where a virtual IBAN is used, there is nevertheless transparency about the actual location of the customer account.

Question for consultation

Q.9 - *Do stakeholders have any views on the suggested approach to ensure more transparency about the location of originator and beneficiary accounts? Are there any issues or concerns?*

PMPG	<p>Whilst the industry would greatly appreciate the harmonisation of account numbers to a proven standard (such as the IBAN based on the ISO 13616 format), its achievement across all jurisdictions would require a costly multi-year “change” project effecting all parties in the payment chain. Furthermore, the country code embedded in the account number allows only the identification of the location of the account-servicing institution, not necessarily the location of the underlying account holder (i.e. in case of non-resident clients).</p> <p>Nonetheless, PMPG agrees with FATF that Financial Institutions and all involved parties rely on accurate disclosure of payment details, including the debtor and creditor information. It is the responsibility of the debtor agent to ensure the correct disclosure of the debtor, while the creditor information depends on the details provided by the payer in the payment instruction.</p> <p>Financial Institutions providing payment services to collection agents must guide their clients on proper formatting of payments. Collection agents, in turn, must instruct their merchants to accurately disclose the account holder, i.e., the collection agent as the creditor and the merchant as the ultimate creditor on invoices/payment requests. The newly-introduced ISO 20022 messages enable the necessary transparency by providing dedicated, structured data elements for all actors in the payment chain.</p> <p>However, it is important to differentiate the use of so-called “virtual accounts” by the nature of the account owner/the creditor (such as a collection agent vs. a corporate customer), as well as the underlying business objective. Those range from simplification of reconciliation, optimization of liquidity management (payment factories), trust agency</p>
------	---

	<p>services (law firm acting on behalf of its customer) to FinTech's offering collection services to merchants as discussed above. It, again, remains the responsibility of the Financial Institution offering virtual accounts to:</p> <ul style="list-style-type: none"> - conduct the full client adoption according to the KYC as per their local applicable regulations (both country of main account and virtual account), - ensure cross-border payments split into (domestic) legs are undergoing the appropriate handling as per their true (cross-border) nature, including compliance filtering, monitoring, central bank/regulatory reporting (e.g., EU VAT directive)
--	--

e. Obligations on beneficiary financial institutions to check alignment of beneficiary information in payment messages (paragraph 20 and 21 of INR.16)

The number and value of fraud cases has grown significantly in recent years, and fraud is now the dominant type of proceeds-generating crime globally, as set out in recent FATF reports². Fraudsters commonly exploit the absence of checks for consistency between account number and account holder name to conceal the true destination of funds, e.g., in push-payment fraud. Fraud involving cross-border payments is particularly problematic given the additional difficulty of cross-border investigations, and of freezing and recovering stolen assets in a cross-border context. Blocking such fraud before payments can be completed is therefore a priority for national authorities. Checks on the consistency of beneficiary information offer the possibility to pause or block many types of fraudulent payments from being completed. Such checks also contribute to making sure that originating and intermediary financial institutions rely on accurate information for transaction monitoring and sanction screening, and such checks are already implemented by some banks and jurisdictions for this reason.

The current requirements of INR.16 state that the beneficiary financial institution should verify the identity of the beneficiary for qualified wire transfers. However, there is no explicit requirement on the financial institution of the beneficiary to verify that the beneficiary information they receive in the payment message aligns with the information they themselves already hold on the beneficiary. The FATF is considering adding requirements for the beneficiary financial institution to check the alignment between the beneficiary information provided by the originating customer, and the verified information of the beneficiary account holder, in order to identify and potentially prevent execution of fraudulent or erroneous transactions. The proposed revisions set out an obligation in paragraph 20 that the beneficiary financial institution should check whether the beneficiary information in the payment message aligns with the information held by the beneficiary financial institution. This is further clarified by the proposed revisions in para 21, which envisage that the beneficiary financial institution should have effective risk-based policies and procedures for determining the follow-up action when the beneficiary information in the payment messages does not align with the information held by the beneficiary financial institutions.

The use of term 'alignment' does not envisage that an exact match is expected in all cases and allows flexibility to countries and financial institutions to apply a risk-based approach to determine the degree of alignment. A risk-based approach would also be applied to determine the appropriate action to be taken, reflecting the risk situation of the jurisdiction or the individual financial institution.

Question for consultation

Q.10 – Do stakeholders support the FATF's proposal? If not, why? Will the proposed obligations help financial institutions in better addressing their financial crimes risks? Does the term "aligns with," together with the risk-based provisions in paragraph 21, create a clear and sufficiently flexible standard? What are potential unintended consequences of this proposal if any? In terms of how financial institutions can meet these requirements more effectively and efficiently, what kind of guidance and information should the future FATF Guidance include? If financial institutions have already implemented these checks, what are the

² Illicit Financial Flows from Cyber-Enabled Fraud, 2023 - <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf>

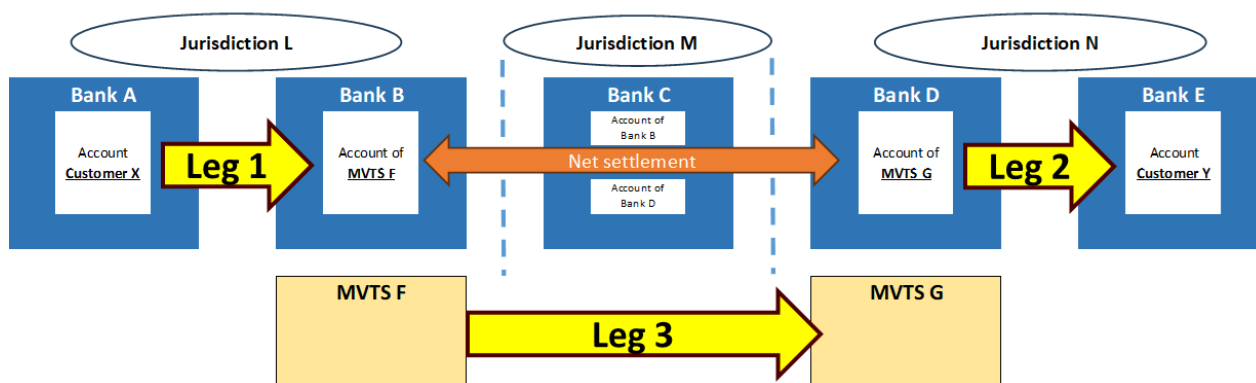
current best practices of implementing the proposed requirements that could be introduced in the future FATF Guidance?

PMPG	<p>The PMPG is unable to support this FATF proposal for the following reasons:</p> <ul style="list-style-type: none"> • The perceived risks associated with the proposal outweigh the benefit in terms of fraud prevention. Concerns primarily revolve around heightened risk to consumer data privacy and protection, potentially leading to identity theft. For instance, there is apprehension that sharing personal details, like name, address and date of birth as part of a payment transaction that would be stored on various systems, could expose individuals to scams, such as those originating from unregulated marketplaces, as evidenced by statistics from the UK. • The proposed measures do not appear to be proportionate to the risk, especially considering that the data transmitted may be unverified. <p>Whilst the PMPG appreciates FATF's efforts to address fraud risks, we suggest exploring alternative methods to manage these risks, rather than solely burdening creditor agents with compliance costs, which are likely to yield suboptimal outcomes.</p> <p>Instead, the PMPG believes that validating the information at an earlier stage would enhance efficiency. The Confirmation of Payee mechanisms and emerging pre-validation models, which enable beneficiary account validation before payment execution, have demonstrated effectiveness in mitigating risk associated with inaccurate or incomplete data.</p>
------	--

f. Definition of payment chain (paragraph 23)

R.16 concerns the information that must be included in instructions along the payment chain. The way the payment chain is defined, therefore, determines the scope of R.16 and which entities have an obligation to comply. The evolution in payment sector structure and business models during the past decades have led to the emergence of new players in the payment ecosystem, and as a result there can be situations in which it is not clear where the payment chain should be considered to begin, and therefore which entities have obligations under R.16. Clarifying the start, intermediary, and end points of payment chains in a way that would be more technology-neutral is essential to achieve the objectives of R.16.

The required originator and beneficiary information must travel the whole length of a cross-border payment, rather than being fragmented among a series of discrete domestic payments, whereas currently, some cross-border payment chains are broken into domestic payments with net settlement in the middle.



MVTS providers are increasingly collecting and disbursing funds through electronic means. The start and end points may not be traditional bank accounts, but also payment accounts, electronic money wallets, or virtual accounts. Payment messages do not go necessarily through SWIFT, and other platforms are increasingly used, for instance for mobile payments. Cross-border payment

chains are often, in effect, broken into two or more domestic transfers, and financial institutions involved may not have the full information on the ultimate originator/beneficiary. This means that often the MVTS or other service providers send wire transfers to other financial institutions without specifying the name of the true originator, and customers may send wire transfers to these providers without specifying the true beneficiary. This may also result in obscuring the jurisdiction of origin or destination, thereby impeding screening and monitoring, as well as supervisory and law enforcement actions. MVTS providers are covered under the definition of 'financial institutions' in the FATF Glossary. In the example above, MVTS F has an obligation to ensure that required information is accompanied in payments or value transfers to MVTS G (subject to the exception of net settlement). MVTS F and MVTS G are also obliged to undertake CDD measures on their customers, in accordance with FATF Recommendation 10.

In addition to the fragmentation of the payment chain (and the information) into several disconnected parts, these market practices, as applied under the current R.16, leave an imbalance in the level of due diligence applied by different actors, with banks expected to apply R.16 in full, while third party payment providers (MVTS in the diagram above) do not apply R.16, arguing that the net settlement exemption applies to those links of the payment chain that are executed by banks. This leaves an unsatisfactory situation in which different market participants carrying out the same economic activity face different rules and different regulatory burdens. Clarifying the start of the payment chain will therefore also help re-establish a level playing field for all financial institutions handling payments.

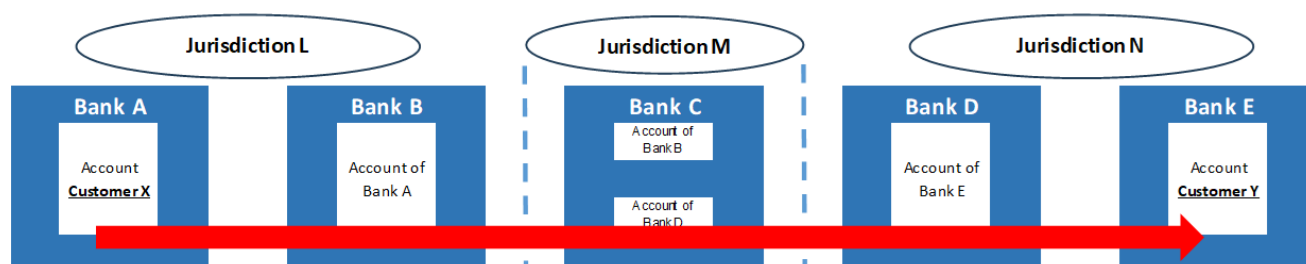
In order to address this fragmentation of payment chains and lack of harmonised implementation and the resulting lack of transparency, the FATF has considered whether a definition of 'payment chain' should be added in INR.16 and what should be the starting point and the end point of a payment. There is also a need to update the requirements to acknowledge the emergence of new payment and messaging methods (other than SWIFT), and new market entrants, so as to follow the principle of "same activity, same risk, same rules", thereby ensuring clear due diligence, transaction monitoring and sanctions screening obligations of the different players in the payment chain, and consistency in regulatory expectations. Two options are being considered in this respect, i.e., whether the payment chain should be considered to begin with the financial institution which receives an instruction from the customer (**Option 1**), or with the financial institution from which, the customer's funds are provided (**Option 2**).

In a large majority of cases, there will not be any difference between these two start-points of the payment chain, as both instruction and funding come through the same financial institution. However, in some cases (e.g. those involving a third-party payment provider), a customer may instruct a financial institution with which they do not hold an account to make a cross-border payment, and provide the funds by drawing on their account with a different financial institution (e.g. using a debit card, or domestic payment channels). In such a situation, Option 1 would consider the third-party payment provider (which receives the instruction) to be the start of the payment chain, while Option 2 would consider the financial institution from which the funds were drawn to be the start of the chain.

Illustrative examples of multiple scenarios (a)-(d)

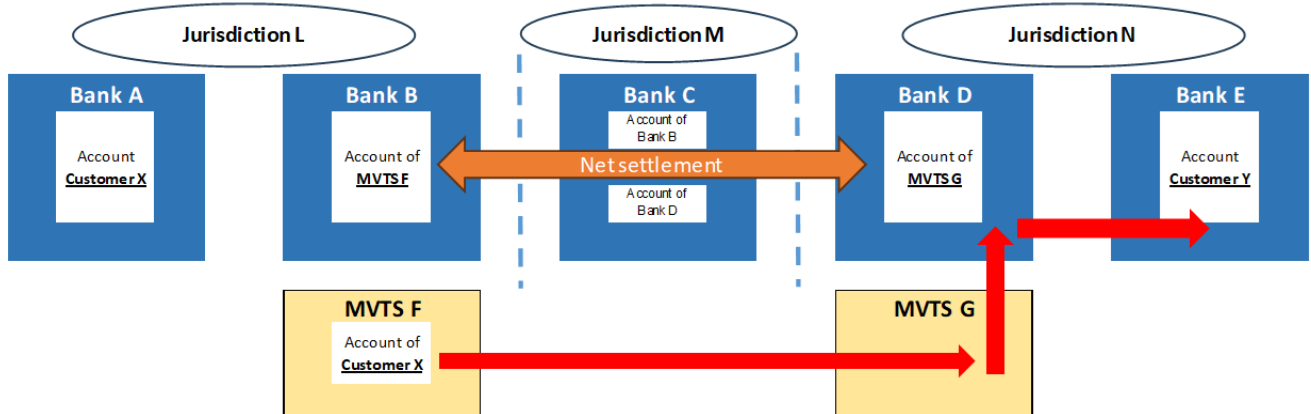
- (a) Customer X with account at Bank A, instructs the Bank to transfer some funds from her/his account to Customer Y with account in Bank E.

Same payment chain routes between Option 1 and 2: Start point is Bank A. All required information should be carried in the payment chain from Bank A to E.



- (b) Customer X with account at MVTS F, instructs the MVTS F to transfer funds from her/his account at MVTS F to Customer Y.

Same payment chain routes between Option 1 and 2: Start point is MVTS F. All required information should be carried in the payment chain from MVTS F ⇒ MVTS G ⇒ Bank D ⇒ Bank E.

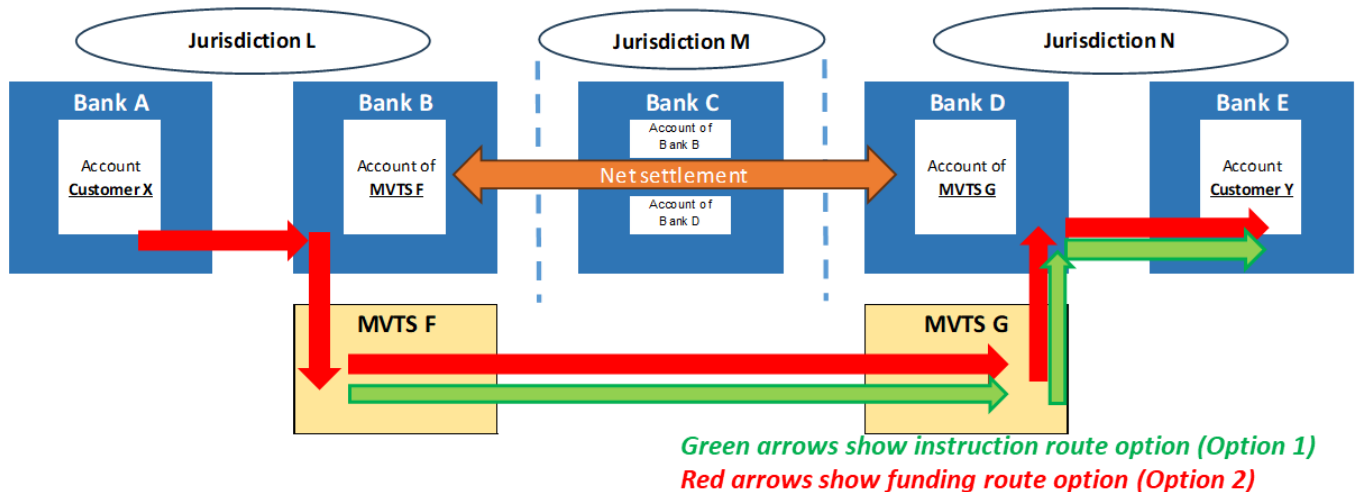


- (c) Occasional Customer X instructs MVTS F to transfer cash. Customer X does not have an account at MVTS F (i.e., the points of receiving an instruction and funds are the same).

Same payment chain routes between Option 1 and 2: Start point is MVTS F. All required information should be carried in the payment chain from MVTS F ⇒ MVTS G ⇒ Bank D ⇒ Bank E.

- (d) Customer X has no account relationship with MVTS F and instructs MVTS F to make a transfer using funds from her/his Bank A account. In this case, funds are automatically withdrawn via debit payment from the connected financial institution (Bank A) upon the instruction to MVTS F (i.e., the points of receiving an instruction and the origin of the funds are different).

Different payment chain routes between Option 1 and 2: In the instruction route option (Option1) Start point is MVTS F. All required information should be carried in the payment chain from MVTS F ⇒ MVTS G ⇒ Bank D ⇒ Bank E. **In the funding route option (Option2)** Start point is Bank A. All required information should be carried in the payment chain from Bank A ⇒ Bank B ⇒ MVTS F ⇒ MVTS G ⇒ Bank D ⇒ Bank E. Even in the funding route, in cooperation with Bank A, MVTS F would be responsible for providing Bank A with the details of the purported transaction (as part of the pull-payment message, or in another workable mechanism), and then for verifying the completeness and accuracy of the message it receives from Bank A through Bank B, and of transferring the message onwards to MVTS G. The rationale of the *funding route* is that Bank A and Bank B would also be aware of the actual nature and beneficiary of the transaction they facilitate, which will help them in identifying attempts to circumvent mitigating measures by using complex payment chains.



Payment transparency if payment chain is considered to start with instruction (paragraph 7(b), footnote 2 of INR.16)

In the event that the start of the payment chain is considered to be the *instruction* (please refer to paragraph 23 of INR.16), a potential gap emerges since the payment message may not include information on the institution and account which is the origin of the funds being transferred (e.g. if the payment chain begins with a third-party payment provider with which the customer does not hold an account). In order to ensure this information is available in the payment message even in such a situation, the revisions propose to add a footnote to paragraph 7 (b) (if a decision is made that the payment chain starts with the customer instruction) to specify that the ordering financial institution should include this information in payment messages. This would mean, with reference to the diagram above, that if MVTS F took payment from the customer drawing on his or her account with a different financial institution, MVTS F would need to include the account number and financial institution that is the origin of funds when taking the payment, in the payment message that it sends to MVTS G.

Questions for consultation:

Q.11 – Do you agree with the issue that FATF has identified with respect to the start of a payment chain and support FATF’s approach to address the issue? The proposed revision (paragraph 23 of INR.16) has two options on whether the payment chain should begin with the instruction by the customer (Option 1), or with the funding (Option 2). Which of the two options would stakeholders prefer for the start of the payment chain and why, also considering the response to question 12 for consultation set out below? What are the aspects where more granular guidance in the future FATF Guidance could be helpful?

PMPG	<p>The PMPG agrees with the principle of Option 1 that the payment starts with the payment initiation and that the information of the originator (= debtor), instructing financial institution (in the sample used ‘MVTS F’ acting as the debtor agent), receiving financial institution (‘Bank E’ = creditor agent) and the beneficiary (= creditor) must travel the whole length of a cross-border payment chain.</p> <p>We also acknowledge the legitimate use of net settlements to transfer liquidity intra- and inter-company across jurisdictions and currencies to enable effective and efficient payment execution. However, where a payment market infrastructure (PMI) is used, it must be ensured only those are selected which facilitate the end-to-end</p>
------	---

	<p>transparency and allow the disclosure of all relevant parties and financial institutions in the payment chain as specified under the Option 1 above.</p> <p>Operators and PMIs must be urged to provide explicit guidelines outlining the acceptable <u>and</u> unacceptable use of their systems based on the payments in scope/out of scope.</p> <p>To ensure compliance with the principle, “same activity, same risk, same rules”, competent authorities must ensure that KYC and account opening controls are required and implemented consistently across all Payment Service Providers (in the example used, banks and MVTSS)</p>
--	---

Q.12 – Do you support the idea of adding footnote 2 of para 7(b) if FATF adopts option 1 above in Q.11? Can the ordering financial institution obtain this information, populate the payment message, and execute the payment? How can this additional information be included in payment messages, e.g., the ISO20022 message? If appropriate data field or messaging system is not currently available, how could this be developed and in what timeframe? Is this footnote clear enough, especially in terms of when and in which cases this requirement applies? Are there any important aspects where the FATF needs to provide more granular expectation in the future FATF Guidance paper?

PMPG	<p>The PMPG does not see the necessity for additional footnotes as the pain.001 message (Request for customer credit transfer initiation) provides appropriate ISO 20022 message fields to drive transparency to the originator’s bank.</p>
------	---

g. Conditions for net settlement (paragraph 24)

The scope of the net settlement exemption is currently covered in footnote 48 (at the end of the glossary that accompanies INR.16) and in paragraph 4 (b) of INR.16. The footnote 48 states: “*It is understood that the settlement of wire transfers may happen under a net settlement arrangement. This interpretive note refers to information which must be included in instructions sent from an originating financial institution to a beneficiary financial institution, including through any intermediary financial institution, to enable disbursement of the funds to the recipient. Any net settlement between the financial institutions may be exempt under paragraph 4(b).*”

Paragraph 4 (b) of INR.16 states that R.16 is not intended to cover the financial institution -to-financial institution transfers and settlements, where both the originator person and the beneficiary person are financial institutions acting on their own behalf.

The current exception for net settlement in INR.16 is in practice being used for a broader range of “account-to-account” transfers, which could undermine the implementation of due diligence requirements by intermediary institutions due to the absence of any information on the underlying transactions, unlike the traditional correspondent banking model. This raises concerns about the effective implementation of targeted financial sanctions obligations, customer due diligence measures and transaction monitoring by financial institutions involved in a payment chain. At the same time, the FATF considers that it is important to preserve the net settlement exemption, where it is relevant, as this can contribute to the provision of small-value remittances at a lower cost and contribute to the objective of financial inclusion.

Clarifying the scope and conditions of the net settlement exception would be an effective way to ensure that requirements are being fulfilled by financial institutions which are parties to the net settlement. This would avoid duplication of obligations and ensure that preventive measures are being applied by financial institutions carrying out transactions on behalf of customers and involved in net settlement.

In the examples above, in any case, MVTS F should send required information to MVTS G in accordance with the newly defined payment chain. However, in the transfers Bank B ⇒ Bank C ⇒ Bank D, intermediary financial institutions that are not included in the payment chain (i.e., Bank B and Bank C) are exempted from the requirement of R.16 in the net settlement cases as long as:

MVTS F needs to conduct CDD on customer X (above the de minimis threshold) and MVTS G needs to conduct CDD on customer Y (above the de minimis threshold). MVTS F and G may rely on agents to conduct CDD, or use third party introduction, or outsource due diligence, as long as they are responsible for the CDD on X and Y and have CDD information, the condition would be met. MVTS F and G are responsible for complying with targeted financial sanctions in their respective jurisdictions for the net settlements. In addition, it is supposed that a net settlement agreement exists in accordance with the definition of ‘MVTS network’ in the Glossary for R.16. Net settlements in which proposed paragraph 24 applies should pay attention to the requirements set out in paragraph 22 (‘take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed’; and ‘should file an STR in any country affected by the suspicious payments or value transfers, and make relevant transaction information available to the Financial Intelligence Unit’).

Question for consultation:

Q.13– *With the clarity on the payment chain (paragraph 23) and paragraph 24, do stakeholders observe any remaining risks associated with net settlement that should be addressed in the R.16/INR.16 amendments? Are there any aspects where FATF should provide more granular expectation in the future FATF Guidance?*

PMPG	As outlined in the response to Question 11, it is imperative for payment market infrastructures (PMIs) to ensure the transmission of the complete information as stipulated in the guidance (Recommendation 16). Therefore, PMI operators, including those adhering to the ISO 20022 standard and particularly those not yet compliant, should proactively identify any necessary enhancements. This will ensure that the required information can be transmitted transparently through the PMI without the risk of data truncation or loss. It is essential for PMIs to emphasize the correct utilization of their systems in alignment with the aforementioned considerations, stressing both the payments in scope and, more importantly, payments out of scope of the PMI.
------	--

h. Financial inclusion, de-risking and other policy consideration such as cost and speed

The proposed revisions seek to ensure that the objectives of financial inclusion and financial integrity are mutually supportive and that the measures taken by jurisdictions are focused and proportionate. Nevertheless, any requirements to provide additional information carry a risk that those who cannot easily provide or verify such information, or for whom the costs of obtaining and verifying this information are too high, may as a result be excluded (or “de-risked”). This would be contrary to the policy intent of both the FATF and the wider G20 programmes on payments, and it is important that we identify and mitigate these risks early. FATF would like to invite stakeholders to highlight any issues or concerns relevant from the financial inclusion perspective related to the proposed amendments and to suggest any alternative approaches or mitigating measures that may be necessary. In addition, the FATF is open to considering further amendments that could enhance financial inclusion and, in particular, the accessibility of payment services and other important policy objectives while ensuring payment transparency and maintaining a level playing field.

In addition to specific issues of financial inclusion or de-risking, the FATF is also supportive of the G20 goal to make payments faster and cheaper, for all customers, and invites views on how the proposals above can support those objectives.

Question for consultation:

Q.14 – Do stakeholders have any views on the proposed revisions to R.16/INR.16 from a financial inclusion perspective, including potential impact on account-opening policy and procedures of financial institutions, and humanitarian considerations? Which, if any, specific proposals raise particular concerns? Are there any alternative approaches or mitigating measures in case of such concerns?

PMPG	Speed of settlement is a top priority of the CPMI cross-border payments program and the industry to respond to customer expectations. Regulations that introduce more friction and cost to payment processes could challenge the G20 objective of achieving faster, cheaper, and more inclusive payments. New requirements should be proportionate to the risk, and be equally applied to all origination and end points to not unintentionally push payments to perceived “faster” methods with less stringent regulation.
------	---

i. Impact on other FATF Recommendations

Question for consultation:

Q.15 – When and how the R.16 revision applies to the virtual assets (VA) sector will be considered separately by FATF. If you are aware of any technical difficulties or feasibility challenges in applying this proposed revision to the VA sector, please specify. FATF will welcome proposals on how to address those difficulties and challenges, if any.

PMPG	<p>PMPG agrees with the overarching objective, emphasizing the importance of tailoring specific recommendations, rather than embedding the complexity of this new sector into R.16 and suggests these initial points for consideration:</p> <ul style="list-style-type: none"> • Virtual Assets/Currencies include Tokenized Securities, Virtual Currencies, Initial Coin Offering (ICOs). • Deposit Tokens: being non-account-based, they require distinct consideration to account-based-requirements. • Distributed Ledger Technology (DLT): require different considerations due the absence of intermediaries. • Hosted and Self-Hosted-Wallets: hosted wallets provide accessible information, while self-hosted wallets pose challenges. • KYC onboarding: while some jurisdictions mandate full KYC onboarding for Virtual Asset Service Providers (VASPs), transaction details may not be transparent due to blockchain limitations. • Central Bank Digital Currencies are the only Virtual Asset which could potentially be considered for inclusion in R.16 due to the issuer being a Central Bank and their secure, controlled nature. <p>By acknowledging these challenges and tailoring recommendations accordingly, we can better address the complexities of the virtual asset sector while upholding overarching objectives.</p> <p>PMPG remains at your disposal for further discussions on this complex subject.</p>
------	---

Q.16 – Do you agree with the proposed changes to the Glossary definitions?

PMPG	Proposed updates to the glossary are included in the glossary section. The PMPG recommends that the ISO terms of ‘debtor’ and ‘creditor’ be adopted in place of ‘originator’ and ‘beneficiary’ given the transition to the ISO 20022 messaging and the clarity that these terms provide.
------	--

j. Timing of implementation of R.16/INR.16 revisions

The timeline for implementation of the proposed revisions of R.16/INR.16 is a key consideration as several proposals rely on the implementation of ISO 20022 and other technical changes, which will only fully come into force in a few years. In this context, responses from stakeholders to the following questions will help the FATF decide the next steps in implementation of the Standards revisions, as agreed.

Normal practice of FATF is that amendments take effect immediately. However, FATF recognises the need for transitional arrangements to enable private sector partners and payment market infrastructures to be adapted and made ready to implement the new requirements in an orderly way, as well as the need to provide further clarifications through Guidance.

Questions for consultation:

Q.17 – Do stakeholders have any views on the timelines for implementation of the proposed revisions to R. 16/INR. 16? What should be the lead time for implementation of the proposed new requirements and why?

PMPG	<p>Regarding the implementation of these recommendations, it is essential to plan for a post-migration phase following the transition to ISO 20022 messaging.</p> <p>ISO 20022 structured and richer messaging serves as the foundation for these requirements, and the earliest possible support for any new mandates would align with the November 2026 Standards Release. The industry and ecosystem require sufficient time to complete the migration and operationalize structured data effectively.</p> <p>Additionally, emphasizing the role and responsibility of payment market infrastructures (PMIs) is crucial. To prevent misuse of clearing systems, PMIs and system operators must clearly define and publish the payments within their clearing scope. Moreover, the payment messaging standard utilized should enable end-to-end transparency by accommodating all necessary data elements to clearly identify all actors involved in a payment. The greatest advantage of ISO 20022 lies not only in its structure and richness, but particularly in its data dictionary, which precisely defines the meaning of each element, role, data type, etc., facilitating automated end-to-end processing, including data interpretation within anti-financial crime compliance processes.</p> <p>Timelines for card would depend on the new requirements and form part of a separate project.</p>
------	---

Q.18 - Are there any issues that should be addressed in the proposed amendments, or wider issues concerning payment transparency, which will require clarification through FATF Guidance?

PMPG	<p>The PMPG stresses the vital role of Payment Transparency in mitigating financial crime risk.</p> <p>However, the current payments landscape is complex, involving numerous actors and operational intricacies not fully addressed in the consultation.</p> <p>Rather than relying solely on traditional payment messaging, we advocate for a holistic re-evaluation of R.16 at a principle level. This entails exploring how payment transparency can harmonize with other controls such as the Customer Due Diligence (CDD), heightened regulatory oversight for non-banking PSPs, and the inclusion of PMI operators in regulatory scope. By adopting a principle-based approach, we can avoid disruptive overhauls to existing payment models, which often lead to increased customer frictions, higher costs, and slower processing times – contrary to the objectives outlined in the G20 Roadmap for Enhancing Cross-Border payments.</p>
------	--

Submission of comments

The FATF recognises that due to the technical nature of this subject, a full consultation will require an ongoing dialogue with the relevant bodies and experts in both public and private sectors. This written consultation is the first step in a wider consultation process, which will also include further discussion and engagement, as needed, informed by the responses to this initial consultation. Please provide responses to this initial consultation by **3 May 2024**.

Please provide your response, including any drafting proposals, and your response to consultation questions set out in the Explanatory Memorandum to FATF.Publicconsultation@fatf-gafi.org with the subject-line "Comments of [author] on the proposed revisions to R.16/INR.16" .

While submitting your response, please indicate the name of your organisation, the nature of your business, and your contact details. Responses to 'Questions for consultation' can be submitted in any format. You may also insert any specific drafting proposals directly in the attached text of the draft revisions in tracked changes. We will use your contact information only for the purpose of this public consultation and for further engagement with you on this issue. Your comments will also be shared with the FATF delegations in the course of this work unless you indicate otherwise. The FATF will, however, not share this information with third parties without your consent.

At this stage, the FATF has not approved the draft revisions to R.16/INR.16 and will consider the feedback received in public consultation for finalising the revisions.

We thank you for your input in advance.

Amendments in the current text of R.16/INR.16 are highlighted in **red and underlined** and deletions in ~~strikethrough~~

Recommendation 16. ~~Wire transfers~~ Payment transparency*

Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire payments or value transfers and related messages. ~~This information should be structured to the extent possible and should that the information~~ remains with ~~the wire~~ such payment or value transfer or related message throughout the payment chain.

Countries should ensure that financial institutions monitor wire payments or value transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measures.

Countries should ensure that, in the context of processing wire payments or value transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing.

Interpretive Note to Recommendation 16 (~~Wire transfers~~ Payment transparency)

A. OBJECTIVE

1. Recommendation 16 ~~has was developed with~~ the objective of preventing terrorists and other criminals from having unfettered access to wire payments or value transfers for moving their funds, and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator and beneficiary⁴⁶ of wire payments or value transfers is immediately available:
 - (a) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, and prosecuting terrorists or other criminals, and tracing their assets;
 - (b) to financial intelligence units for analysing suspicious or unusual activity, and disseminating it as necessary, and
 - (c) to ordering, intermediary and beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions, and to implement the requirements to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001) relating to the prevention and suppression of terrorism and terrorist financing.
2. To accomplish these objectives, countries should have the ability to trace all wire payments or value transfers. Due to the potential terrorist financing threat posed by small wire payments or value transfers, countries should minimise thresholds, while taking into account the risk of driving transactions underground and the importance of financial inclusion. It is not the intention of the FATF to impose rigid standards or to mandate a single operating process that would

⁴⁶ The terms "originator" and "beneficiary" are used in Recommendation 16 and its Interpretive Note. These terms are interchangeable with the terms "debtor" and "creditor" respectively, which are used in certain messaging standards such as ISO 20022.

negatively affect the payment system.

B. SCOPE

3. Recommendation 16 applies to cross-border and domestic wire payments or value transfers ~~and domestic wire transfers~~, including serial payments, and cover payments.
4. Recommendation 16 is not intended to cover the following types of payments:

Option 1 – Requiring issuing and acquiring bank information

- (a) Any transfer that flows from a transaction carried out using a credit or debit or prepaid card for the purchase of goods or services from merchants, so long as the credit or debit or prepaid card number, as well as the name and location of the issuing and acquiring financial institutions⁴⁷, accompanies all transfers flowing from the transaction. However, when a credit or debit or prepaid card is used ~~as a payment system~~ to effect a person-to-person wire payment or value transfer, the transaction is covered by Recommendation 16, and the necessary information should be included in the message.

Option 2 – Exclude withdrawals, purchases of cash and a cash equivalent

- (a) Any transfer that flows from a transaction carried out using a credit or debit or prepaid card for the purchase of goods or services from merchants, so long as the credit or debit or prepaid card number, as well as the name and location of the issuing and acquiring financial institutions [footnote 47], accompanies all transfers flowing from the transaction. ~~However, when a credit or debit or prepaid card is used as a payment system to effect a person-to-person wire transfer, the transaction is covered by Recommendation 16, and the necessary information should be included in the message.~~
However, Recommendation 16 does apply in situations:
 - when a credit or debit or prepaid card is used ~~as a payment system~~ to effect a person-to-person wire payment or value transfer; or
 - when a credit or debit or prepaid card is used to make a cross-border withdrawal or purchase of cash or a cash equivalent; or
 - when a credit or debit or prepaid card is used to make a domestic withdrawal or purchase of cash or a cash equivalent with a value over USD/EUR 1000
 - (b) Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are financial institutions acting on their own behalf.
5. Countries may adopt a de minimis threshold for cross-border wire payments or value transfers (no higher than USD/EUR 1,000), below which the following requirements should apply:
 - (a) Countries should ensure that financial institutions include with such transfers: (i) the name of the originator; (ii) the name of the beneficiary; and (iii) an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer.
 - (b) Countries may, nevertheless, require that incoming cross-border wire payments or value transfers below the threshold contain required and accurate originator information.

⁴⁷ Card issuer and merchant acquirer information should make it possible for all institutions and authorities referred to in paragraph 1 to identify which financial institutions are in possession of the full cardholder and merchant information, and in which countries these institutions are located.

6. Information accompanying cross-border and domestic payments or value transfers should be structured, to the extent possible, in accordance with the established standards of the system used such as ISO 20022, and should be sufficiently detailed to enable identification of the originator and beneficiary.

PMPG	<p>To avoid any misunderstanding, may we suggest stressing the importance of the Market Infrastructure/Scheme Management and Clearing System Operator and the related rulebooks to clearly document and publish the payments in scope of the related clearing system.</p> <p>The lack of clarity of the payments in scope and out of scope of a clearing system lead to its misuse. Payment Market Infrastructures/System Operators must take responsibility and ensure the payment messaging standard used facilitates the provision of end-to-end transparency by enabling all necessary data elements to clearly define all actors participating in payment (for the payments in scope). The biggest benefit of ISO 20022 is not only its structure and richness, but specifically the data dictionary, which precisely describes the meaning of an element, role, data type, etc. and enables automated end-to-end processing, including data analytics as part of the anti-financial crime compliance processes.</p>
------	---

C. CROSS-BORDER QUALIFYING **WIRE PAYMENTS AND VALUE TRANSFERS**

Option 1 – limited mandatory elements for both originator and beneficiary and additional elements for originator, with optionality

- 6 7. Information accompanying all qualifying wire payments or value transfers should always contain:

- (a) the full name of the originator and beneficiary;

PMPG	<p>Full name requires more precise definition (e.g., full legal name?); whilst this could be achieved for the originator (debtor) by the debtor agent populating the name as captured during the CDD, the full legal name could become a challenge for the beneficiary i.e. often known and provided by the originator by its brand name (e.g. Bayerische Motoren Werke AG = BMW).</p>
------	--

- (b) the originator account number [*footnote 1*] of the originator and beneficiary where such an account is used to process the transaction. In the absence of an account, a unique transaction reference number should be included, which permits traceability of the transaction [*footnote 2*];

[*footnote 1] The account number or the associated payment message data should enable the institutions and authorities referred in paragraph 1 to identify the financial institution and the country where the account holder's funds are located.

[*footnote 2] In cases where the origin of the funds is a financial institution other than the ordering financial institution, the account number and financial institution which is the origin of the funds should be included.

PMPG	<p>Whilst the industry would greatly appreciate the harmonisation of account numbers to a proven standard such as the IBAN based on the ISO 13616 format, its achievement across all jurisdictions would require a costly multi-year "change" project effecting all parties in the payment chain. Furthermore, the country code embedded in the account number allows only the identification of the location of the account servicing institution, not necessarily the location of the underlying account holder (i.e. in case of non-resident clients).</p> <p>The PMPG understands the motivation for this FATF recommendation results from concerns raised on the use of virtual accounts.</p> <p>Considering the issuer of virtual accounts is an adopted and authorised customer of a Financial Institution and the owner of the account including the asset (cash) rather than an intermediary, we recommend FATF to call out the need for the provision of transparency</p>
------	---

	<p>on the underlying business relationship. This would require the 'virtual account owner' to identify the party serviced (i.e. the underlying merchant serviced by a collection agency or the business entity of the customer in case of a POBO/COBO set-up) using the dedicated data element ultimate creditor/ultimate debtor in the respective ISO 20022 message. These do require the identification via name and address with the minimum of country code and town name.</p>
--	--

- (c) ~~the originator's address of the originator and beneficiary, or national identity number, or customer identification number⁴⁴, or date and place of birth or, in the absence of an address, the country and town name; and~~
- (d) ~~or where the originator is a natural person, the national identity number, or a unique official identifier, or the customer identification number⁴⁸, or date and place of birth of the originator;~~

<p>PMPG</p>	<p>Recommendation as an alternative option for FATF's consideration:</p> <p>Financial Institutions should uniquely identify all financial institutions and legal persons in a payment in a standardized and internationally recognized manner.</p> <p>Information accompanying all qualifying payments or value transfers should always contain:</p> <ul style="list-style-type: none"> (a) the full name of the originator and beneficiary or, where the originator and/or beneficiary is a legal person, then the published Business Identifier Code (BIC) (*<i>footnote (1)</i>), and (b) the account number (**<i>footnote (2)</i>) of the originator and beneficiary where such an account is used to process the transaction. In the absence of an account, a unique transaction reference number should be included, which permits traceability of the transaction, and (c) the address of the originator and beneficiary, or, in the absence of an address, the country and town name; (*<i>footnote (1)</i>) <p>Where necessary to achieve unambiguous identification, the originating PSP is encouraged to include additional information such as:</p> <ul style="list-style-type: none"> (d) where the originator is a natural person, the date and place of birth of the originator,
-------------	---

~~⁴⁴The customer identification number refers to a number which uniquely identifies the originator to the originating financial institution and is a different number from the unique transaction reference number referred to in paragraph 7. The customer identification number must refer to a record held by the originating financial institution which contains at least one of the following: the customer address, a national identity number, or a date and place of birth.~~

⁴⁸The customer identification number refers to a number which uniquely identifies the originator to the originating financial institution and is a different number from the unique transaction reference number referred to in paragraph 7. The customer identification number must refer to a record held by the originating financial institution which contains at least one of the following: ~~the customer address,~~ a national identity number, or a date and place of birth.

	<p>or</p> <p>(e) where the originator is a legal person, the published Business Identifier Code (BIC), or the Legal Entity Identifier (LEI) (<i>***footnote (3)</i>).</p> <p><i>* footnote (1) Where structured identifiers are used, internationally recognized Business Identifier Codes (BIC) is a valid alternative to Name and Address, provided that the Name and Address information associated with the identifiers in the directory aligns with the Name and Address that would otherwise be supplied.</i></p> <p><i>**footnote (2) The account number or the associated payment message data should enable the institutions and authorities referred in paragraph 1 to identify the financial institution and the country where the account holder's funds are located.</i></p> <p><i>***footnote (3) "Under ISO 9362, the BIC contains the two-letter ISO country code where the entity is located enabling country level sanction screening on the BIC level without retrieving the related reference data. In the case of LEI, any country identification requires retrieval of the reference data. Depending on the technical set-up of the screening process this could be deemed less efficient".</i></p>
--	---

And where the originator and/or beneficiary is a legal person, the published business identifier code (BIC), or the Legal Entity Identifier (LEI), or the unique official identifier of the originator and/or beneficiary.

PMPG	<p>We understand the value of internationally recognised identifiers, such as the Business Identifier Code (BIC) or the Legal Identifier Code (LEI). However, we see limited benefits of any local official identifiers. For a local identifier to be meaningful to the receiver of an instruction in another jurisdiction, access to the underlying database, the scheme management etc. would be required, which is hardly achievable across 195 countries. The investment required to enable the provision of the data would by far outweigh the very limited potential benefits.</p> <p>Please note: the published BIC, unlike the LEI, identifies the Business Entity including its address in the payment and therefore qualifies as a substitute for name and address. Given the BIC is used for routing of payments in the payment chain, to avoid the provision of conflicting information we strongly suggest recommending the use of BIC <u>or</u> Name and Address and LEI.</p>
------	---

~~(d) the name of the beneficiary; and~~

~~(e) the beneficiary account number where such an account is used to process the transaction.~~

Option 2 – full alignment in mandatory elements between originator and beneficiary

6 7. Information accompanying all qualifying wire payments or value transfers should always contain, for both the originator and beneficiary:

(a) the full name of the originator;

(b) the originator account number [**footnote 1*] where such an account is used to process the transaction. In the absence of an account, a unique transaction reference number should be included, which permits traceability of the transaction [**footnote 2*];

[*footnote 1] The account number or the associated payment message data should enable

the institutions and authorities referred in paragraph 1 to identify the financial institution and the country where the account holder's funds are located.

[*footnote 2] In cases where the origin of the funds is a financial institution other than the ordering financial institution, the account number and financial institution which is the origin of the funds should be included.

- (c) the originator's address, or national identity number, or customer identification number [FN44], or date and place of birth or, in the absence of an address, the country and town name; and
- (d) or where the originator and/or beneficiary is a natural person, the national identity number, or a unique official identifier, or the customer identification number [footnote 48], or date and place of birth of the originator and/or beneficiary;

PMPG	In addition to all arguments under 6(d) above, considering requesting this level of data for the beneficiary is impossible to achieve, such requirements are likely to increase the risk for P2P payments to be settled via alternative channels/provider.
------	--

- (e) and
- (f) where the originator and/or beneficiary is a legal person, the connected business identifier code (BIC), or the Legal Entity Identifier (LEI), or the unique official identifier of the originator and/or beneficiary.
- ~~(d) the name of the beneficiary; and~~
- ~~(e) the beneficiary account number where such an account is used to process the transaction.~~

~~7. In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.~~

8. Where several individual cross-border wire payments or value transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they may be exempted from the requirements of paragraph 6.7 in respect of originator information, provided that they include the originator's account number or unique transaction reference number (as described in paragraph 7 above), and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

D. DOMESTIC WIRE PAYMENTS AND VALUE TRANSFERS

9. Information accompanying domestic wire payments or value transfers should also include originator information as indicated in paragraph 7 for cross-border wire payments or value transfers, unless this information can be made available to the beneficiary financial institution and appropriate authorities by other means. In this latter case, the ordering financial institution need only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.

10. The information should be made available by the ordering financial institution within three business days of receiving the request either from the beneficiary or intermediary financial institution or from appropriate competent authorities. Law enforcement authorities should be able to compel immediate production of such information.

E. RESPONSIBILITIES OF ORDERING, INTERMEDIARY AND BENEFICIARY⁴⁹ FINANCIAL INSTITUTIONS

Ordering (debtor) financial institution

11. The ordering financial institution should ensure that qualifying wire payments or value transfers contain required and accurate originator information, and required beneficiary information.
12. The ordering financial institution should ensure that cross-border wire payments or value transfers below any applicable threshold contain the name of the originator and the name of the beneficiary and an account number for each, or a unique transaction reference number.
13. The ordering financial institution should maintain all originator and beneficiary information collected, in accordance with Recommendation 11.
14. The ordering financial institution should not be allowed to execute the wire payments or value transfer if it does not comply with the requirements specified above.

Intermediary financial institution

15. For cross-border wire payments or value transfers, financial institutions processing an intermediary element of such chains of wire transfers should ensure that all originator and beneficiary information that accompanies a wire payment or value transfer is retained with it.
16. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire payment or value transfer from remaining with a related domestic wire payment or value transfer, a record should be kept, for at least five years, by the receiving intermediary financial institution of all the information received from the ordering financial institution or another intermediary financial institution.
17. An intermediary financial institution should take reasonable measures to identify cross-border wire payments or value transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing.
18. An intermediary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire payment or value transfer lacking required originator or required beneficiary information; and (ii) the appropriate follow-up action.

Beneficiary (creditor) financial institution

19. A beneficiary financial institution should take reasonable measures to identify cross-border wire payments or value transfers that lack required originator or required beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible.
20. For qualifying wire payments or value transfers, a beneficiary financial institution should (i) verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with Recommendation 11 and (ii) check that the beneficiary information in the payment messages aligns with the information held by the beneficiary financial institution.
21. A beneficiary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire payment or value transfer lacking

⁴⁹ The terms "ordering financial institution (s)" and "beneficiary financial institution (s)" are used in Recommendation 16 and its Interpretive Note. These terms are interchangeable with terms "debtor agent" and "creditor agent" respectively, which are the terms used in certain messaging standards such as ISO 20022.

required originator or required beneficiary information or when the beneficiary information in the payment messages does not align with the information held by the beneficiary financial institution; and (ii) the appropriate follow-up action.

PMPG	<p>As stated in our response to question 9, the PMPG does not support the new requirement around alignment.</p> <p>However, if this change is approved, further clarity is sought regarding the term “alignment”. It does not clearly articulate the expectations that will be placed on the creditor agent/beneficiary financial institution regarding alignment of beneficiary information and the treatment of payments that are not aligned. Lack of clarity may result in an influx of blocked payments, in many cases where there is no actual money laundering or financial crime risk associated (these could be payments that have been processed successfully for years). The timing of the application of this requirement also needs clarification, particularly concerning whether it should be applied pre-or post-processing. Clear guidelines are needed on the level of reliance Financial Institutions should place on unverified information received with the payment instructions.</p> <p>These concerns are expected to significantly impact customers, introducing more friction and cost to payment processes, which could contradict the G20 objective of achieving faster and cheaper payments.</p>
------	---

F. MONEY OR VALUE TRANSFER SERVICE OPERATORS

22. Money or value transfer service (MVTs) providers should be required to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents. In the case of a MVTs provider that controls, or is part of a MVTs network controlling, both the ordering and the beneficiary side of a wire payment or value transfer, the MVTs provider:
- should take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and
 - should file an STR in any country affected by the suspicious wire payments or value transfer, and make relevant transaction information available to the Financial Intelligence Unit.

G. PAYMENT CHAIN AND NET SETTLEMENT

Option 1 (instruction route)

23. For purposes of implementation of Recommendation 16, the payment chain starts at the financial institution that receives the instructions from the originator for transfer of funds to the beneficiary. The end point of the payment chain is the financial institution that services the account of the beneficiary or remits cash to the beneficiary.

Option 2 (funding route)

23. For purposes of implementation of Recommendation 16, the payment chain starts at the financial institution that either holds the account of the originator, or receives cash from the originator. The end point of the payment chain is the financial institution that services the account of the beneficiary or remits cash to the beneficiary.

24. The settlement of payment or value transfers may happen under a net settlement arrangement. This interpretive note refers to information which must be included in instructions sent from an ordering financial institution to a beneficiary financial institution, including through any intermediary financial institution, to enable disbursement of the funds to the recipient. Any net settlement between the financial institutions (e.g. banks, MVTs or MVTs networks) may be exempt under paragraph 4(b) which covers financial institution-to-financial institution transfers and settlements, where both the originator and the beneficiary are financial institutions acting on their own behalf. Where any net settlement results from qualifying payments or value

transfers transactions carried out on behalf of customers, parties to the net settlement should be required to apply CDD measures to their customers for such underlying transactions and to comply with applicable targeted financial sanctions.

Glossary of specific terms used in this Recommendation

Account Number	Refers to the account identification or account proxy that the account servicing Financial Institution assigns to the account
Accurate	is used to describe information that has been verified for accuracy.
<u>Address</u>	<u>refers to the physical location of a residence or business. For a business, the address should be a registered address.</u>
Batch transfer	is a transfer comprised of a number of individual wire payments or value transfers that are being sent to the same financial institutions, but may/may not be ultimately intended for different persons.
Beneficiary	refers to the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire payments or value transfer <u>in a chain of payments or value transfers</u> . Equivalent Terms are Creditor or Payee. Note: An Ultimate Creditor might be referenced in the payment if the Creditor receives the payment on behalf of another party.
Beneficiary Financial Institution	refers to the financial institution <u>that services the account of the beneficiary or remits cash to the beneficiary. The beneficiary financial institution is the end point in a payment chain, which receives the wire transfer from the ordering financial institution directly or through an intermediary financial institution and makes the funds available to the beneficiary.</u> Equivalent Term is Creditor Agent.
Connected Business Identifier Code	<u>BIC refers to a universal business identifier code based on the ISO 9362 standard assigned to financial and non-financial institutions and corporates.</u> <u>Connected BICs are those used by financial institutions and eligible corporates, for instance to access the SWIFT network.</u>
Cover Payment	refers to a wire payment or value transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution (the direct message) with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.
Cross-border wire payment or value transfer	refers to any wire payment or value transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer payments or value transfers in which at least one of the financial institutions involved is located in a different country.
Crypto asset account	An account held by a crypto-asset service provider in the name of one or more natural or legal persons and that can be used for the execution of transfers of crypto-assets;
Crypto asset	A digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology;

Crypto-asset service	Any of the following services and activities relating to any crypto-asset: (a) providing custody and administration of crypto-assets on behalf of clients; (b) operation of a trading platform for crypto-assets; (c) exchange of crypto-assets for funds; (d) exchange of crypto-assets for other crypto-assets; (e) execution of orders for crypto-assets on behalf of clients; (f) placing of crypto-assets; (g) reception and transmission of orders for crypto-assets on behalf of clients; (h) providing advice on crypto-assets; (i) providing portfolio management on crypto-assets; (j) providing transfer services for crypto-assets on behalf of clients.
Crypto-asset service provider	'provides 'crypto-asset services'
Domestic wire payment or value transfers	refers to any <u>wire payment or value transfer</u> where the ordering financial institution and beneficiary financial institution are located in the same country. This term therefore refers to any chain of <u>wire transfer payments or value transfers</u> that takes place entirely within the borders of a single country, even though the system used to transfer the payment message may be located in another country. The term also refers to any chain of <u>wire transfer payments or value transfers</u> that takes place entirely within the borders of the European Economic Area (EEA) ⁵⁰ .
Financial Institution	Refers to any regulated payment service provider that provide fund transfers, to include credit transfers, direct debit, money remittances whether domestic or cross-border, and transfers carried out using a payment card, an electronic money instrument, mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics.
Intermediary financial institution	refers to a financial institution in a <u>serial or cover</u> payment chain that receives and transmits a <u>wire payment or value</u> transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution. Equivalent Term is Intermediary Agent.
Legal Entity Identifier	<u>refers to a unique alphanumeric reference code based on the ISO 17442 standard assigned to an entity by the Global LEI System.</u>
Merchant	<u>refers to any business (conducted by a natural or legal person), professional, non-profit organisation, or public sector entity associated with the regular provision of goods and services, which was onboarded by the relevant financial institution as such, following the required CDD in respect of such activity. This excludes natural persons acting as consumers.</u>
MVTS network	<u>refers to any or a combination of the two following elements: (i) an MVTS and its agents, or (ii) two or more MVTS bound by one or several agreements to proceed to payments or value transfers, including but not limited to the net settlement of those transfers.</u>
Ordering financial	refers to <u>[the financial institution that receives the instructions from the originator for transfer of funds to the beneficiary. The ordering</u>

⁵⁰ An entity may petition the FATF to be designated as a supra-national jurisdiction for the purposes of and limited to an assessment of Recommendation 16 compliance.

institution	<p><u>financial institution is the start point of the payment chain.]</u> Equivalent Term is Debtor Agent.</p> <p><u>Note: the ordering financial institution is the Debtor Agent in credit transfers, whereas it is the Creditor Agent in direct debits and in requests to pay, and the acquirer in card transactions</u>the financial institution which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.</p>
Originator	<p>refers to the account holder who <u>allows requests</u> the <u>wire payment or value</u> transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the <u>wire payment or value</u> transfer.</p> <p>Equivalent terms are:</p> <ul style="list-style-type: none"> • Debtor or Payor for credit transfers; • Creditor or Payee for requests to pay, direct debit, card payments and any other form where the order is placed by (or on behalf of) the payee. <p><u>Note: An Ultimate Debtor/Creditor might be referenced in the payment.</u></p>
Qualifying wire payments or value transfers	<p>means a cross-border <u>wire payments or value</u> transfer above any applicable threshold as described in paragraph 5 of the Interpretive Note to Recommendation 16.</p>
Required originator and/or beneficiary information	<p>refers to the information elements set out in subparagraphs 7(a)-(e). is used to describe a situation in which all elements of required information are present. Subparagraphs 6(a), 6(b) and 6(c) set out the required originator information. Subparagraphs 6(d) and 6(e) set out the required beneficiary information.</p> <p><u>Note: Except for account information, referenced ultimate parties will be required to carry the same required information.</u></p>
Serial Payment	<p>refers to a direct sequential chain of payment where the <u>wire payments or value</u> transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g., correspondent banks).</p>
Straight-through processing	<p>refers to payment transactions that are conducted electronically without the need for manual intervention.</p>
Unique official identifier	<p><u>refers to an identification scheme that is issued by the public sector in the relevant jurisdiction and that ensures that a given identifier refers to a unique person, entity or legal arrangement, and that a given person, entity or legal arrangement only has one identifier in that scheme.</u></p>
Unique transaction reference number	<p>refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the <u>wire payments or value</u> transfer.</p>
Ultimate creditor	<p><u>Represents a party that is the ultimate beneficiary of the payment. For example, the payment is credited to an account of a financing company, but the ultimate beneficiary is the customer of the financing company.</u></p>
Ultimate debtor	<p><u>Represents a party that originally ordered goods/services and to whom the seller has sent the invoice. Ultimate debtor is used when the receiver of the invoice is different from the originator.</u></p>

Wire Payment(s) or value transfer	refers to any transaction carried out on behalf of an originator through an <u>ordering</u> financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person . ⁴⁶ <u>[This includes cash withdrawals and deposits when cash is provided by or deposited to an institution different from the one holding the account (for that purpose, a head office and cross-border branch are considered to be different institutions).]</u>
Self-hosted address	A distributed ledger address not linked to either of the following: (a) a crypto-asset service provider; (b) an entity not established in the Union and providing services similar to those of a crypto-asset service provider;
Transfer of crypto-assets	'Any transaction with the aim of moving crypto-assets from one distributed ledger address, crypto-asset account or other device allowing the storage of crypto-assets to another, carried out by at least one crypto-asset service provider acting on behalf of either an originator or a beneficiary, irrespective of whether the originator and the beneficiary are the same person and irrespective of whether the crypto-asset service provider of the originator and that of the beneficiary are one and the same;
Utility Token	utility token' means a type of crypto-asset that is only intended to provide access to a good or a service supplied by its issuer;
Asset-referenced token	asset-referenced token' means a type of crypto-asset that is not an electronic money token and that purports to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies;

~~⁴⁶— It is understood that the settlement of wire transfers may happen under a net settlement arrangement. This interpretive note refers to information which must be included in instructions sent from an originating financial institution to a beneficiary financial institution, including through any intermediary financial institution, to enable disbursement of the funds to the recipient. Any net settlement between the financial institutions may be exempt under paragraph 4(b).~~