



April 26, 2024

Ms. Violaine Clerc
Executive Secretary
Financial Action Task Force (FATF)
2 Rue André Pascal 75116
Paris, France

RE: Public Consultation on the draft FATF R.16/INR.16 amendments

Dear Ms. Clerc,

The Wolfsberg Group (“the Group”) appreciates the opportunity to provide comments on the draft Financial Action Task Force “FATF” amendments to Recommendation 16 “R.16” and its interpretative note “INR.16”. We are supportive of FATF’s efforts to update R.16 to ensure relevance in today’s payments ecosystem and to level the playing field across all actors involved in the movement of payment or value, irrespective of the nature of those stakeholders and whether or not they are banks.

Today, where one actor’s position in ensuring payment transparency starts and ends is no longer as clear-cut as when cross-border payments (outside of those made in cash) moved almost entirely through regulated banks via Swift messages. Regardless of the various new and emerging payment methods, the Group stands by the principle **that a payment is a payment**, and as such the ordering payment service provider (PSP) – bank or non-bank – has the obligation to ensure that a new payment is structured appropriately, clearly identifying the debtor and creditor in any transfer of funds.

The Group has always viewed payment transparency as a foundational element to an effective financial crime compliance programme. However, the modern payments world has become more complex, involving multiple payment actors and complex operating models, than this R.16 consultation considers. There is no “one size fits all” approach and rather than trying to cover all payment scenarios, we believe that it would be more effective for FATF to adopt **a principles-based approach** to R16 and consider other financial crime risk management controls such as customer due diligence, enhanced regulatory supervision for non-bank PSPs, clarification of roles and responsibilities of each PSP in the payment chain, in mitigating the risks set out in the proposed draft. This principles-based approach would minimise subjecting users of cross-border payments to excessive data intrusion, which could translate into increased customer friction, higher cost and slower processing times and be at odds with the G20’s objective of “making cross-border payments faster, cheaper, more transparent and more inclusive.” This approach would also avoid the re-engineering of the existing payments ecosystem and deliver results that are more proportionate to the desired outcomes.

The challenges associated with payment transparency cannot be resolved solely by payments and compliance specialists within banks, but rather require agreement among all stakeholders in the payments ecosystem – including competent authorities, the operators of countries’ payment market infrastructures (PMI), and non-bank PSPs that provide payments – to understand how accountability for payment transparency is distributed across the financial system appropriately, such that the overarching principle of **“same activity, same risk, same rule”** is implemented in both regulation and supervision. This is aligned to the workstream led by the Financial Stability Board under the G20’s Roadmap for Enhancing Cross Border payments on “bank vs. non-bank supervision” which seeks to



address any regulatory/supervisory inconsistencies or barriers and resultant impact on cross border payments.

We strongly recommend that FATF bring operators of PMIs into the scope of R.16 as they are key enablers of payment transparency requirements by making possible the inclusion of relevant payment data. We recommend for operators of PMIs and the relevant competent authority(ies) to identify appropriate technological enhancements, ISO20022 standards preferred, to facilitate evolving payments and settlements adequately. In addition, PMIs should specifically address, in a consistent way, the degree to which the PMI permits intermediated payments and how such payments (including the payment parties) should be captured according to the PMI's message format – including specifying types of transactions not permitted to be channelled through the PMI. The PMI rulebook should also clearly state the compliance obligations of the debtor, intermediary and creditor PSPs in their relationship with the PMI.

The Group notes FATF's rationale in not adopting **ISO 20022 terminology** but recommends revising the terminology used in R.16 to align to ISO 20022 and be "future proofed" as adoption of, and adherence to, ISO 20022 standards increases. A glossary/footnote can be attached to cross reference the ISO20022 terms to the "old" terminologies. We also recommend that FATF employ terminology that can be applied broadly across the financial services industry, including new market entrants which may or may not be regulated to the same degree as traditional banks. As such, Financial Institutions (FIs) should be referred to as "payment service providers" (PSPs) and, in line with ISO 20022 lexicon, the ordering FI is defined as the "debtor agent PSP", the intermediary FI as the "intermediary agent PSP", and the beneficiary FI as the "creditor agent PSP" – agnostic to whether the underlying entity or "agent" is a bank or non-bank FI (NBFi). In the same vein, the use of "MVTs" terminology by FATF also has the possibility of being misinterpreted innocently or wilfully. We recommend that FATF take the approach that a 'payment is a payment' and rather than refer to FIs and MVTs, they should instead refer to all entities that offer a service that involves cross border movement of funds.

The above highlights the Group's overarching comments on R.16 while the next section provides a detailed response to each of FATF's consultation questions for your consideration.

As ever, the Group is grateful for the opportunity to comment on the draft changes to R.16/INR.16 and would like to thank you in advance for your consideration of our feedback. We remain at your disposal should any clarification be necessary.

Yours sincerely,

Alan Ketley
Executive Secretary
The Wolfsberg Group

Detailed Response

Seq.	Question	Wolfsberg Group Response
1.	<i>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?</i>	We support FATF's objective to mitigate financial crime risk associated with card payments. However, the typologies listed in the explanatory memorandum for R.16 do not establish a clear link between the card payment risk typologies and the purchase of goods and services exemption. As presented, the typologies appear to fall within the purview of other FATF Recommendations (notably R.10) related to Customer Due Diligence (CDD), given that the card issuers and deposit-takers in question are subject to those CDD laws and regulations. The most effective way to manage the financial crime risks presented by the typologies cited remains Anti-Money Laundering/Counter Terrorist Financing (AML/CTF) and sanctions compliance measures, not by increasing the data accompanying the transfer. Using one of the typologies listed by FATF as an example, where the use of shell companies to open offshore bank accounts with merchant acquiring banks accepting credit/debit card charges for illicit goods purchased, we would suggest that the most effective way to mitigate this risk is through enhanced regulation for FIs, e.g. raising the minimum CDD standards at merchant acquiring institutions, and thus effectively limiting the ability of shell companies to operate accounts. Furthermore, even with greater payment transparency, the FIs will still have no visibility over the actual goods being purchased so it is unclear what benefits these changes would drive in mitigating the risk presented by the typologies identified in the beginning of this section. For example, if a customer purchases materials that have heightened risk concerns from a legitimate online retailer, passing additional data fields between the card issuer and the online retailer's bank will still not identify what goods the card was actually used to pay for. A better and more effective way to manage payment card risk is to look at the underlying CDD obligations on the issuers and acquirers. For that reason, we would question both options, but will address them separately below. However, we would also like to note that debit and credit card transactions afford a level of visibility which cash transactions do not and there is a risk that changes here could drive the types of transactions referred to in the risk typologies into cash transactions, which could hamper the efforts of law enforcement further. It is our view that irrespective of the use case, whenever a card is presented (physically or online), or at an ATM, the real-time card authorisation process links up the merchant terminal with the card issuer through the card network, (e.g. Visa or MasterCard), and the settlement that follows remains the same with built-in transparency of the issuing and acquiring institutions. As such, the transparency of such type of payments is greater than a non-cards funds transfer. Option 1 (Card exemptions): proposal to include additional information i.e. name and location of the issuing and acquiring FIs to accompany the transfer. Greater clarity is needed for Option 1 in terms of roles and responsibilities of the multiple FIs and card scheme operators involved. Furthermore, we note that the only entities to see the entire end-to-end payment flow and parties involved (i.e. the card issuer, settlement banks, merchant acquirers, beneficiary banks) are the card scheme operators. Additionally, the funds flow settlement is done in bulk and separate from the actual transaction. Clarification will be needed from FATF in terms of the roles and responsibilities of each payment

Seq.	Question	Wolfsberg Group Response
		actor in the chain, considering how the card schemes operate. Finally, we do not see how the addition of the card issuer and merchant acquirer details would improve FI's financial crime detection or risk mitigation capabilities. Option 2: We do not support the proposal for the lifting of exemptions for the purchase of cash and cash equivalents. Withdrawal of cash/cash equivalents would fall within the "access to own funds" exemption and removing the 'withdrawal or purchase of cash or cash equivalent' calls into question the applicability of the access to own funds principles, which could have much broader consequences in terms of costs and impact on consumers. The participants in the transactions need to be clearly identified: in this case it is unclear who would be the payer and who would be the beneficiary, given that customers are accessing funds from their own accounts. There also needs to be a clearer definition of what constitutes a cash equivalent. Does it include: all tokens that can be converted to fiat cash, prepaid including gift cards, gambling chips, air miles which can be converted to a fiat equivalent, or transacting with a crypto exchange? Option 2 also entails significant infrastructure and process changes, including message and format changes, requiring these transactions to be passed through screening and message testing. As a result, payment costs would increase and there could be delays to payments given the need to screen and resolve any sanctions hits that the additional information might create. This would also entail moving away from the model of immediate access to a customer's own funds, while providing minimal, if any, improvements to financial crimes detection or mitigation. Financial crime risks associated with cash withdrawals should instead be addressed through CDD measures. For example, if a customer banks in jurisdiction A and withdraws cash in jurisdiction B in order to deposit it in jurisdiction B, the holder of the account in jurisdiction B would still be subject to the CDD requirements in jurisdiction B, which would include applicable cash controls/cash deposit limits, as well as transaction monitoring. This change would have a material impact on expatriate workers, corporate travellers and holiday-makers being able to access their own funds. It could also have a disproportionate impact to customers with foreign names which may not easily conform to western language convention and are likely to face heightened name matching challenges and delays when trying to access their own funds overseas. In addition, we note that banks have in place cash monitoring controls and will know that their account holder is accessing cash overseas through a specific code assigned to cash withdrawals. Recommendation: We do not support Option 2. Banks must allow customers to withdraw their cash while in foreign jurisdictions. There is no third-party transfer involved in a debit card withdrawal or purchase of cash or cash equivalents as a debit card transaction is a demand to pull their own funds from a known debit account via a debit card, duly issued credit card, or a prepaid card. Including foreign ATM withdrawals in the scope of R.16 would have substantial adverse impacts to customers traveling outside their home country, should access to their own funds be temporarily delayed or prohibited. For Option 1, we would recommend that FATF clarify the roles and responsibilities for each of the FIs involved in the card settlement and set out how the addition of both data points will help FIs with their financial crime obligations. Without this clarification, we are unable to make an informed assessment of whether we are supportive of Option 1. We urge FATF to work with card networks to obtain visibility

Seq.	Question	Wolfsberg Group Response
		into Bank Identification Number (BIN) lists as needed for use in their investigations and law enforcement activities. This would cause minimal disruption to payments processing. To address the stolen card fraud typologies mentioned in the explanatory memorandum, we would suggest stronger collaboration between card networks and FIs to develop fraud prevention and reporting capabilities. Crucially, we urge FATF to continue to support and amplify the message of “same activity, same risk, same rule” to supervisors globally. All FIs, whether banks or non-bank financial institutions (NBFIs), involved in the movement of value/payment should be subject to the same AML/CTF regulations. For example, FIs that issue or support stored value cards should be subject to the same regulatory standards as a fully regulated bank, proportionate to their activity. This would align better to the Financial Stability Board (FSB)-led workstream under the G20’s Roadmap for Enhancing Cross Border Payments on “bank vs. non-bank supervision” set up to develop recommendations, as needed, to promote supervision of banks and non-banks that is consistent with the differences in risks that they pose, including the regulatory/supervisory inconsistencies or barriers and their impact on cross border payments.
2.	<i>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?</i>	<u>Payment Instrument Agnostic</u> • Limiting the exemptions to credit, debit and prepaid cards constitutes too narrow a view and does not bring the whole payment ecosystem e.g. e-wallet payments, within the scope of the payment transparency principles. Rather, by focusing narrowly on card payments, consumers may turn to other non-card payment methods, e.g. e-wallets or cash, for their purchases of goods and services. This poses the risk of driving transactions to more opaque methods. Without a consistent framework, the risk may simply move from traditional payment methods into alternate payment methods for which there may be no consistency of regulatory oversight or application of FATF Recommendations, leading to greater ML/TF risks. • We urge FATF to adopt a neutral definition in their exclusion of transactions used for purchase of goods and services. This is aligned to the European Funds Transfer Regulation 2015/847, Para (13) which broadens the exclusion of purchase of goods and services to cover all other forms of payment methods and not just card payments. • In addition, in line with the principles of “same activity, same risk, same rule”, it is key that all FIs that are involved in the acquiring of payment transactions, whether traditional acquiring models structured around the use of payment cards, or different business models, are all obliged entities and subject to equivalent principles as those applicable to card transactions and traditional wire transfers. This stance is consistent with the European Payment Service Directive 2015/2366, Para. 10 • This is critical to the effectiveness of financial crime risk management across the payments ecosystem. Imposing greater obligations on traditional payment structures (making them slower and more costly for customers) risks driving usage into the areas where the requirements are lesser and, therefore, more opaque. <u>Recommendation:</u> To add the statement in red below to INR 16, Para 4(a). “Recommendation 16 is not intended to cover the following types of payments: Any transfer that flows from a transaction carried out using a payment card, electronic money instrument, mobile phone or other digital or information technology (IT) prepaid or post-paid devices with similar characteristics, for the purchase of goods or services.....”

Seq.	Question	Wolfsberg Group Response
3.	<i>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?</i>	This will be dependent on the Payment Market Infrastructure (PMI) used for the card payments and the way in which those transactions are settled interbank. We do not see from the typologies listed in R.16 how the addition of the card issuer and merchant acquirer details would improve financial crime detection or risk mitigation capabilities, particularly given the potential impact to existing card messaging systems.
4.	<i>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?</i>	We support FATF's proposal to apply the amended card exemption equally to credit, debit, and prepaid cards. Nonetheless, we would note that the risks for debit and credit cards should be considered separately to prepaid cards, as pre-paid cards are more analogous to cash transactions than they are to debit and credit cards. While certain prepaid cards, e.g. anonymous, open network, reloadable, may present a higher level of ML/TF risks, the risk mitigating controls should not be under the purview of R.16 but rather through other stricter regulatory requirements and oversight on the issuance of such cash-like instruments e.g. limits, transaction monitoring. Debit and credit card transactions provide a level of transparency which cash transactions do not – there is a risk that changes here will drive the types of transactions referred to in the risk typologies into cash transactions, which could hamper the efforts of law enforcement further. Given that, even with greater payment transparency, the FIs will still have no visibility over the actual goods being purchased, it is unclear what benefit these changes would drive in mitigating the risk typologies identified in the beginning of this section. For example, if a customer purchases materials that have heightened risk concerns from a legitimate online retailer, passing additional data fields between the FI card issuer and the online retailer's bank will still not identify what goods the card was actually used to pay for. A better and more effective way to manage payment card risk is to look at the underlying KYC obligations on the credit and debit cardholders and merchants. Many of the risk typologies listed at the beginning of this section appear to flow from know your customer principles for both the originator's FI and the end beneficiary's FI. Recommendation: FATF should adopt a neutral stance and extend the existing card exemptions to cover all electronic payments for the purchase of goods and services. To add the statement in red below to INR 16, Para 4(a):

Seq.	Question	Wolfsberg Group Response
		Any transfer that flows from a transaction carried out using a payment card, electronic money instrument, mobile phone or other digital or information technology (IT) prepaid or post-paid devices with similar characteristics, for the purchase of goods or services.....". Please refer to Question 2 for further details. Although we advocate parity on transparency requirements across payment methods, there are unique concerns around the utilisation of prepaid cards, and we would advocate for stricter regulatory requirements and oversight on the issuance of such cash-like instruments. In order that the higher risks of cash usage be better addressed, we also recommend a renewed focus on rules for cash acceptance, for example as is currently envisaged under draft EU AML Regulation proposals.
5.	<i>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?</i>	Please refer to Question 2's response.
6.	<i>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 be differentiated according to card type? Should it apply only to withdrawals above a threshold and if so, what is</i>	Please refer to Question 1's response. In addition, in the case of cash withdrawal, there is no third-party transfer of funds. It is the cardholder interacting with the ATM to provide the necessary authentication credentials to facilitate the withdrawal. A cardholder presents their card at an ATM, the card is validated and the transaction authorised in real-time. The originator and beneficiary are the same. Notwithstanding the above, we do not consider there to be a payment transparency gap in the current card authorisation and settlement model managed by the card networks. Our view is that irrespective of the use case, whenever a card is presented either physically at a merchant location or at an ATM, or virtually on an online marketplace, the authorisation process and the settlement that follows remain the same and have built-in transparency of the issuing and acquiring institutions.

Seq.	Question	Wolfsberg Group Response
	<i>the appropriate threshold?</i>	
6bis.	<i>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?</i>	As per our responses to Question 1 and 6, we believe that R.16 should not apply to cash withdrawals: these represent a core ability for customers to access their own funds. Risks here should be addressed through CDD principles and transaction monitoring, rather than through any revisions to R.16. It would be beneficial to understand the linkage between the typologies and risks presented in the explanatory memorandum vs. the proposed measures. At present, it is unclear what risks could be mitigated through the potential lifting of the exemption on purchase of cash and cash equivalents.
7.	<i>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?</i>	Yes, FATF should clarify what constitutes a cash equivalent in the revisions to R16. As currently proposed, the definition is too broad and will leave room for misinterpretation. This could create confusion with the existing use of the term 'cash equivalent' to denote near cash assets like treasury bills, commercial paper, other liquid assets, prepaid including gift cards or commodity assets. We would also like to understand whether the intention is to include all tokens that can be converted to fiat cash and whether the definition would extend to gambling chips, air miles which can be converted to a fiat equivalent, transacting with a crypto exchange, crypto gift cards, crypto payment cards, closed, or open loop for tokens.
8.	<i>Would stakeholders support FATF's approach</i>	We understand the desired outcome of this proposal is to 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. However, the ability

Seq.	Question	Wolfsberg Group Response
	<i>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?</i>	for FIs to place reliance on this information, specifically on the beneficiary information, is greatly reduced as the information is obtained from the originator and thus unverified. Unless the originating FI can rely on the information, they may decide to continue to rely on requests for information (RFIs) to the beneficiary FI which holds the beneficiary's CDD records in order to discount alerts, thus negating any benefits to automated processing. Relating to draft 7(d), we note that PMIs are not designed to transmit Personal Identifiable Information (PII) and unless addressed appropriately, this requirement exposes originators' and beneficiaries' PII to all parties in the payment flow, creating heightened risks of data theft and leaks. We do not support this proposal; however, should it be maintained in the revised R16, FATF will need to address this newly created risk and provide guidelines as to how it is envisaged that such PII information be collected and handled by FIs and PMIs. For both proposed options, we would highlight that any additional data points proposed will have an operational and infrastructure impact, both from the perspective of data point capture and the PMI's ability to pass on the additional data. Specifically for (b), certain PMIs do not use ISO200022 standards or lack the technical infrastructure to include all necessary payment data. Therefore, PMIs will need to uplift their existing infrastructure progressively before this proposal can achieve its desired outcome. The below outlines our specific stance on Option 1 and 2. <u>Option 1:</u> Originator and Beneficiary name FATF must provide guidance on what is meant by "full name of originator and beneficiary" as this can be open to interpretation. The 2023 Wolfsberg Payment Transparency Standards include guidance on address conventions, which FATF may find useful. Originator and Beneficiary address For the originator's address, we support FATF's proposal to make the originator address a mandatory requirement and would recommend that FATF remove the optionality for FIs to put in only the country/town name of originator's address. The address of the originator should be as verified or identified during the CDD process by the originator FI, in accordance with applicable laws and regulations. We understand that having the beneficiary's full address may be helpful and represents best practice. However, this information is unverified and does not address the fact that certain individuals may not have a fixed place of abode (financial inclusion). As such, we advocate for the inclusion of beneficiary address as best practice only, not mandatory, to avoid unintended consequences e.g. rejection or querying of beneficiary information by originating or intermediary FIs. It is relevant to note that the account domicile geography can be deduced from the location of the beneficiary bank e.g. BIC country code from the payment message. Additionally, there are challenges that will emerge if beneficiary address is made mandatory such as: • Data quality issues due to reliance on the originator to provide the beneficiary's address. • Inability of the originator and originating institution to verify the accuracy of the beneficiary address.

Seq.	Question	Wolfsberg Group Response
		- Impact on straight-through-processing and efficiency of payment processes if the beneficiary's address is a mandatory data point. Considering the potential for data quality issues, the impact could be significant. Originator's ID number, unique official identifier or the customer identification number, or date and place of birth: Not Supportive - Any additional data points, especially PII such as ID number, and DOB, will present trade-offs i.e. data protection, privacy, identity theft. Sending PII in a payment message will expose the originator to higher risks of data leaks/impersonation. We believe these risks far outweigh the benefits of any financial crime mitigation. PMIs have not been designed to transmit PII information. Moreover, as an example, US Licensed Money Transmitters are not subject to the same regulatory standards that govern their use of third party service providers and vendors. As a result, this leaves consumers vulnerable to weaker financial and data privacy protection where unlicensed entities, such as a technology service provider, are involved in the funds transfer process. Unless data privacy and protection are addressed with robust rules and regulations, this may have broad unintended consequences and unfairly penalise the originator. - We do not see the projected efficiency in identification of the originator. Based on today's practice, the presence of ID number/unique official identifier would be of limited benefit until all financial crime and sanctions lists are required to contain this information. If this additional data point is included in those lists and there is trust in the data, then this will generate the efficiency in identification that FATF is hoping for. We note that for sanctions alert generation, place of birth is not used as a data point as one's place of birth is not of relevance from a fair customer treatment perspective. Originator and/or beneficiary to include the BIC/LEI, or the unique official identifier: Supportive as a principle In general, we are supportive of the principle of including an LEI/BIC or unique official identifier to enhance the accuracy of identification information on relevant parties. In recognition that the current LEI adoption is mainly confined to large corporates in highly developed economies, we recommend that FATF make suitable allowances for a transition period for entities to adopt LEI. We believe that requiring LEI usage too soon will result in friction in global payments and raise financial inclusion barriers particularly for small and medium sized enterprises in less developed economies. In addition, similar to the point raised above, there needs to be a corresponding push from FATF for list providers and relevant authorities to populate such BIC/LEI or unique official identifier information in their lists to maximise the effectiveness of requiring, and subsequently using, this information. As an example, from feedback given to us by third party vendors, a significant part of the challenge is to tie, definitively, the name on the LEI lists to a name on the sanctions list. <u>Option 2:</u> We do not support Option 2 as the information on the beneficiary is unverified and hence FIs may decide not to rely on that information and may continue to go via the RFI route. In addition, the introduction of this data point comes at a potential cost to customer experience (e.g. slower processing times due to additional data collected) and exposing them to heightened risk of data theft, impersonation, data privacy and protection. Overall, we also note that certain PMIs are unable to carry this additional data on originators/beneficiaries and would need to upgrade their infrastructure before this change could be implemented. It is also unclear what is meant by making the information available to

Seq.	Question	Wolfsberg Group Response
		beneficiary FI “by other means” and if it applies to all payments. We recommend not using alternative information transmission arrangements on a regular basis as this fragments payment information.
9.	<i>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?</i>	The current R.16 draft lacks a clear definition of virtual IBAN (vIBAN). Equally, the term “vIBAN” appears to imply a specific subset of products/services when FATF’s intention may be to address concerns across a broader base of products/services that share similar attributes. In addition, we recognise that the use of such products/services can vary depending on the type of customer using the product/service and the use case and/or payment flows being supported. As such, we request further clarification from FATF on the below: 1. Definition of vIBAN, which is key to help the industry identify what is in/out of scope. For example, vIBAN can be used in a variety of ways, such as for reconciliation of accounts used by corporates, collection agents, electronic money institutions and other FIs. Furthermore, the term “vIBAN” is a Europe centric terminology and would recommend that it be replaced with “virtual reference number.” This is a neutral term, defined in the <u>Wolfsberg Payment Transparency Standards</u> as “A virtual reference number – also at times referred to as “virtual account number”, “virtual International Banking Account Number (vIBAN)”, “virtual identification number”, “virtual receivables number” or “virtual bank account” – is a reference number issued by a PSP to allow the tracking of incoming payments. A unique bank account may have multiple virtual reference numbers linked to it. A virtual reference number is typically linked to a unique bank account.” The virtual reference number should reference the IBAN and failing which, it should be passed on in the payment message, to the fullest extent possible by the PMI. 2. Given that a vIBAN can be used in a multitude of ways, we would like to understand how FATF envisages the role of each FI involved in the vIBAN payment/value transfer, specifically since no FI will be able to have the full end to end view. For example, in the case of a collection agent model, only the FI that issues the vIBAN will know that it is virtual (it will look like any other IBAN to other parties in the payment flow). There is no “one size fits all” model, and it would be helpful if FATF could walk through several working examples of how a vIBAN is used and the ability of FIs to be able to identify categorically that the vIBAN can enable the identification of the FI and the country where the account holder’s funds are located. This problem cannot be solved unilaterally by mandating that the payment message data identify the FI and the country where the account holder’s funds are located. Additionally, the inclusion of an account number alone also does not provide this transparency to other FIs in the payment chain. From an originating bank’s perspective, when payment instructions are received from their customers to send funds, the FI cannot reliably ascertain with certainty the country where the beneficiary account holder’s funds are located from the account number alone. In addition, even if their customer were to inform the originating FI of the country where the beneficiary account holder’s funds are located within the payment message data, there is a dependency on the originating FI, and all other FIs in the payment chain, on the PMIs in both the sending and receiving jurisdiction having the capacity to pass/receive the full payment message. Responsible use of vIBAN can, in certain instances, increase payment transparency compared to non-vIBAN “omnibus” or pooled funds type accounts, as they can be segregated and allocated to underlying individual customers. <u>Recommendations:</u>

Seq.	Question	Wolfsberg Group Response
		We recommend FATF to adopt the term “virtual reference number”, as defined in the Wolfsberg Payment Transparency Standards. FATF and relevant competent authorities should encourage PMIs to identify appropriate technological enhancements, ISO20022 preferred, and support the consistent and correct population of data via adoption of structured message fields, as such enhancements are reasonably practicable. Further, PMIs should clearly document and publish the payments in scope of the related clearing system in their rulebooks. They should also provide sufficient guidance on payment messaging standards used to facilitate the provision of end-to-end transparency, by enabling the provision of all relevant data elements required to define all relevant actors participating in a given transaction. This can be through enhancements to payments and/or messaging systems to add structured fields or character space to capture intermediary FIs and additional message information related to cross-border payments, bundled payments, or payments associated with the purchase of goods or services, or to accommodate indicators for domestic payments that originated cross-border. These technological enhancements are indispensable for there to be effective payment transparency. As set out in our Wolfsberg Payment Transparency Standards, beneficiary FIs have an obligation to instruct their customers on the appropriate usage of vIBAN when giving settlement instructions to counterparties, e.g. to ensure that when vIBANs are allocated to specific parties, those counterparties do not replace the true account beneficiary (e.g. in merchant acquiring or collection “on behalf of” scenarios). Beneficiary FIs must define and establish appropriate usage of vIBANs, in line with the standards and rules of relevant PMIs and competent authorities and instruct their clients on the appropriate usage accordingly. Furthermore, they should apply a risk-based approach to ensure that their customers are using vIBANs as intended, including the application of appropriate controls (e.g. account activity review) to manage the risks of non-compliance. Likewise, FIs issuing vIBANs should ensure that appropriate controls are in place to populate the relevant vIBAN details in outbound payment message data for transactions originated by their customers, to the fullest extent possible by the PMI.
10.	<i>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</i>	We do not support FATF's proposal for the below reasons: 1. The risks far outweighed the benefits of any fraud prevention. Specifically, we are concerned with the heightened risks that consumers will have to face in term of data privacy and protection that increases the risk of identity theft. For example, John (a fraudster) goes onto Facebook marketplace and makes an offer to buy a shirt from a legitimate seller. The unsuspecting seller may then pass on his personal details upon request from John claiming that this is to fulfil payment transparency requirements, i.e. name, address, DOB, in order for John to send the money to the seller. John takes the information and sells it on the Dark Net. Note that in the UK, a significant number of scams occur within unregulated marketplaces. 2. As above, we are not at all supportive of this proposal. Should it go ahead, however, we would need to have our understanding confirmed by FATF, that beneficiary FIs are able to apply risk-based policies and procedures and to take remedial actions on misalignment of information ex post.

Seq.	Question	Wolfsberg Group Response
	<i>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 current best practices of implementing the proposed requirements that could be introduced in the future FATF Guidance?</i>	We believe this proposal, if implemented, will have significant impact from a customer standpoint, increasing friction and cost to settlement and is clearly at cross-purposes with the G20 objectives of faster and cheaper settlement. The measures proposed do not appear to be risk proportionate, especially where the data transmitted are unverified. <u>Recommendation:</u> We welcome FATF's efforts to address fraud risks and indeed, this is an area of concern globally. However, we recommend that FATF consider other means to manage the fraud risk e.g. Confirmation of Payee, rather than placing the cost of compliance solely on the beneficiary FI, achieving a sub-optimal outcome at best. The UK, for example, has implemented domestic measures specifically designed to tackle fraud e.g. shared reimbursement model, delaying outbound payments for up to 4 working days when fraud is suspected, looking at liability/refunds. Such measures have been undertaken outside of payment transparency requirements and we would recommend that the same approach be taken, rather than including disproportionate amendments to R.16.
11.	<i>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</i>	We note and welcome FATF's effort to enhance payment transparency and address fragmentation of payment chains by clarifying the start and end of a payment. Option 1: Instruction route – Supportive in principle with conditions We agree with the principle of instruction route (Option 1) that the payment starts with the payment initiation and that the payment information of the originator, ordering FI, beneficiary, and beneficiary FI needs to be transmitted in full. We note that this will depend on the availability of domestic/local PMIs e.g. ACH/Real Time Payments, having the right infrastructure to carry the full information through to the last leg of the payment. <u>Recommendations for Option 1</u> For reasons mentioned above, we support Option 1 in principle with the below conditions. 1. FATF to recommend that PMI operators and the relevant competent authority(ies) clearly document and publish the payments in scope of the related clearing system in their rulebooks. Further, PMIs must take responsibility to enhance payment infrastructure and ensure the payment messaging standards used, ISO20022 preferred, facilitate 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) to be present. Competent

Seq.	Question	Wolfsberg Group Response
	<i>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?</i>	authorities should encourage domestic/local PMIs to have the right infrastructure to carry the full payment information for this cross-border purpose and to provide sufficient guidance for the appropriate use of payment data fields. This goes to the principle of “same activity, same risk, same rule.” This is also aligned to the FSB led workstream under G20 Cross Border payments on “bank vs. non-bank supervision” which seeks to understand more on the regulatory / supervisory inconsistencies or barriers and their impact on cross border payments.” 2. In the context of the payment diagram provided in the explanatory memorandum, we would like to confirm our understanding that Intermediary FIs (Banks, B, C or D) do not have any obligation to conduct CDD on customer X and Y as they are not customers of theirs. Option 2: Funding route – Not supportive We are not supportive of Option 2. How a customer chooses to fund/pay for a payment can be different from who is “making” the payment, e.g. a corporate client funding treasury accounts for payments, or an individual funding his wallet periodically and then deciding at a later date to instruct his bank to make a remittance overseas. We stand by the principle that the payment starts with the payment instruction (and not funding) as if this principle does not stand, it will quickly become overly complex and unwieldy to implement. In addition, using the FATF example given, Bank A would not be aware in any scenario that the transaction is travelling internationally hence would be unaware of the requirements placed to provide any additional information other than what the domestic clearing system would mandate. Similar to Option 1, we note the limitation of the domestic rails and inconsistencies across the domestic and cross border payment platforms. In addition, we note a logical inconsistency in the description of the funding route – if alignment is required on the beneficiary side of the transfer, then why would it not also be required for the FI to confirm alignment of the information on the funding account with the information on the account itself? This could be because the FI does not have information beyond the account number but the risk on identifying the funding source is the same as for paying funds to the beneficiary. We are concerned that subsequent impact of this draft amendment (Option 2) would inadvertently disrupt legitimate business models of new service providers, raise the cost of cross-border payments contrary to the G20 goals, and undermine regulatory efforts to foster competitiveness, risking the G20 objective of inclusion.
12.	<i>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?</i>	Clarification: We would require further clarification on Footnote 2 before we can provide an informed opinion as to whether we would support Footnote 2. We also note that it is not practical for an originator to know/seek to know whether the beneficiary holds a payment account relationship with its FI or not. As such, we understand that this requirement refers to the FI of the originator only, not the beneficiary, and given language in R16, the text references the origin of funds and not the destination of funds. 1. Origin of funds: is FATF referring to the ultimate payer (Customer X) or is it referring simply to the FI (Bank A) from where the funds are coming? If the former, the proposal may not be feasible for all scenarios, e.g. the example of a card payment made by Customer X, the settlement will be done via card schemes and Bank B will only see a bulk payment from a third-party payment processor, and not the underlying payer. Only MVTs F will see the full information because the originator will need to have entered the full details of the transaction into the MVTs’ systems. We also note that many non-payment account holding FIs operate using business

Seq.	Question	Wolfsberg Group Response
	<i>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?</i>	models that entail the bundling of payments being transmitted through one or more intermediary FIs. In these instances, it is not feasible to unbundle these flows to carry individual originator details (and by extension the funding FI details) throughout the payment chain, without considerably increasing costs for the market and importantly, consumers. 2. As above, certain domestic/local PMIs' have limited ability to carry the full payment information. 3. Further clarity is required and context, including a robust risk mitigation rationale, is strongly recommended should Footnote 2 be added to the INR R.16. As it reads today, it can be easily misinterpreted or overlooked completely.
13.	<i>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?</i>	Refer to Question 11's response under Recommendations. We would also like to point out a misconception in section G that MVTS G will perform CDD on Customer Y. This would not be the case if Customer Y is merely the beneficiary of the domestic payment from MVTS G. CDD on Customer Y will be performed exclusively by Bank E. We recommend that FATF consider the different levels of risks posed by bulk, or bundled, or batched transfers if they are as applicable to one-to-many, many-to-one, and many-to-many. The reference to batched files in para. 8 of the proposed R.16 draft applies to the one-to-many bundled or bulked payment scenario. Recommendation: R.16 and subsequent FATF guidance should provide clarity on net settlements/bulk/bundled/batched transfers involving the many-to-many scenario, which is the prevailing use case for third party cross border payments.

Seq.	Question	Wolfsberg Group Response
14.	<i>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?</i>	Access to own funds – Option 2 proposal to remove “withdrawal or purchase of cash or a cash equivalent” to be excluded from R.16 exemption will be in contravention with the “access to own funds” principle. It would also have a disproportionate impact to customers with foreign names which may not conform to western language convention easily and are likely to face heightened name matching challenges and delays when trying to access their own funds overseas.
15.	<i>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.</i>	We believe that the first level principles on payment transparency should apply equally to both fiat and virtual assets payment/value transfer. This harmonisation is key to ensure a level playing field and that there is no regulatory arbitrage to be gained. We support FATF’s proposal to come up with separate guidance on how payment transparency principles can be applied on virtual assets transfers. This should be done with the support of an expert working group, with members who have deep subject matter expertise on virtual assets and fiat transfers.
16.	<i>Do you agree with the proposed changes to the Glossary definitions?</i>	a) Accurate: FATF: “is used to describe information that has been verified for accuracy”

Seq.	Question	Wolfsberg Group Response
		Suggested wording: “is used to describe information that has been verified.” b) Address: FATF: “refers to the physical location of a residence or business” Suggested wording: “refers to: • For a natural person, a residential or business street address; • For a legal person (such as a corporation, partnership or trust), a principal place of business, local office or other physical location” c) Cross border payment or value transfer: FATF: “refers to any <u>wire payment or value transfer</u> where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of <u>wire-transfer payments or value transfers</u> in which at least one of the financial institutions involved is located in a different country.” Suggested wording: “refers to any payment or value transfer where at least one of the debtor agent PSP, intermediary agent PSP, creditor agent PSP is located in a different country.” This is cleaner and covers all scenarios including intermediary PSP. d) Domestic payment or value transfers FATF: “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).” Suggested wording: “refers to any payment or value transfer where the debtor agent PSP, intermediary agent PSP, creditor agent PSP 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).” e) Payments or value transfer FATF: “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 <u>person</u> at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same <u>person</u>.⁴⁶ <u>[This includes cash withdrawals and deposits when cash is provided by or deposited</u>

Seq.	Question	Wolfsberg Group Response
		<u>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> Suggested wording: We recommend removing “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).” This is at odds to why it is included in the definition of a payment(s) or value transfer and recommend that it be removed. f) Cover payment We recommend aligning the current definition to Swift, i.e. “A cover payment is sent by or on behalf of the ordering institution directly, or through correspondent(s), to the financial institution (account servicer) of the beneficiary institution. It must only be used to order the movement of funds related to an underlying customer credit transfer.”
17.	<i>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?</i>	Any operational impact and timelines will be dependent on the outcome of this consultation and an industry wide end to end assessment will need to be performed. In addition, given the significant transparency benefits which will be derived from the mandatory roll-out of ISO20022 standards by November 2025, as well as the concomitant structural demands placed on industry actors, including PMIs, in the interim, we would advocate for implementation at a suitable time after the ISO20022 deadline.
18.	<i>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?</i>	• We believe in the principles of Payment Transparency and how critical they are to managing financial crime. However, the modern payments world is much more complex, involving multiple payment actors and complex operating models, than this consultation considers. Rather, than trying to solve this in a traditional payment message way, we recommend that FATF revisit R.16 at a principles level, and how PT principles can be achieved in conjunction with other controls e.g. CDD, enhanced regulatory supervision for NBFIs, bringing Payment Market Infrastructure (PMI) operators into scope etc. This avoids causing major disruption and total re-engineering to the existing payments model, which will translate into increased customer friction, higher costs and slower processing times for consumers, all of which are at odds with the G20 Roadmap for Enhancing Cross- Border Payments, which sets quantitative targets to lower costs, increase speed, accessibility and transparency of international payments by the end of 2027. • We suggest that the opening paragraph of the revised R.16 be amended as follows to provide greater clarity and set expectations accordingly. “Countries should ensure that all payments service providers and asset transfer managers such as financial institutions, Money Service Bureaus, Credit Card Companies etc. include required and accurate originator information, and required beneficiary information, on payments or value transfers and related messages. This information should be structured and passed on to the extent possible and should remain with such payment or value transfer or related message throughout the payment chain.”

