Brussels, 2 May 2024
rV

EACB draft response to the FATF consultation on Recommendation 16

May 2024

The **European Association of Co-operative Banks** (EACB) is the voice of the cooperative banks in Europe. It represents, promotes and defends the common interests of its 26 member institutions and of cooperative banks in general. Cooperative banks form decentralised networks which are subject to banking as well as cooperative legislation. Democracy, transparency and proximity are the three key characteristics of the cooperative banks' business model. With 2,700 locally operating banks and 40,000 outlets co-operative banks are widely represented throughout the enlarged European Union, playing a major role in the financial and economic system. They have a long tradition in serving 227 million customers, mainly consumers, retailers and communities. The co-operative banks in Europe represent 89 million members and 720,000 employees and have a total average market share of about 20%.

For further details, please visit www.eacb.coop

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

General Comments

The EACB welcomes the consultation on FATF Recommendation 16, its Interpretive Note (R.16/INR.16) and the related Glossary of specific terms.

We acknowledge the importance of updating Recommendation 16 to reflect evolutions in payment business models and messaging standards, while still observing the 'same activity, same risk, same rules' principle.

We are however of the view that Recommendation 16 primarily deals with questions that are already part of the European Union (EU) and national legal frameworks, the risk-based approach, the Customer Due Diligence (CDD) practices and the Know Your Customer (KYC) procedures. We wish to highlight that such wide-ranging guidelines, which aim at reducing financial crime risks at transaction level, may lead to more bureaucracy, technical challenges and higher costs for financial institutions, without necessarily resulting in a significant improvement in crime prevention or AML quality. It might be more effective to address and evaluate issues at the customer level instead.

The proposed changes give rise to additional specific concerns that we discuss in the in the corresponding sections below. Our members want to ensure that the proposed revisions take into account practical challenges and perspectives faced in wire transfers.

EACB answers to the FATF consultation on Recommendation 16

a. Terminology changes

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

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?

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?

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?

EACB answer:

- **Q.1:**

We understand that FATF aims to further reduce financial crime risks. **However, we believe that there is a better and more effective way than suggested by both options 1 and 2, namely by ensuring that in this area the customer due diligence measures are applied**

by all PSPs. In addition, we believe that a reduction in the exemptions for card payments with real-time verification could lead to critical unintended consequences in such sensitive use-cases as paying for services and goods or/and withdrawing cash (at ATMs or at POS). Especially when consumers perform these transactions abroad they are highly vulnerable in case of payment delays or payment interruptions. As a result, trust in card payments could erode and consumers and merchants might feel the need to shift to other means of payments which are less secure – not least from an AML/CFT point of view (e.g. stronger reliance on cash carry-on in cross-border settings). We also question the effectiveness of delays or rejections of cash withdrawals through real-time checks during the withdrawal process to combat money laundering. Criminals would first receive information about investigations or arrest risks and immediately initiate countermeasures to obfuscate. Ultimately, questions arise about the security of sensitive customer data transmitted by European card issuers to banks, ATM operators or even merchants with cash-back services in third countries (and not to the new AML authority) if this data includes the name, date of birth and address of tourists or business travellers.

Against these general considerations and the following more detailed remarks, we would even go as far as suggesting not to reduce the exemption, but option 1 is clearly to be preferred over option 2.

Whilst we support the objective pursued by the FATF to enhance the transparency and security of electronic payments, **we suggest limiting Option 1 to payment instruments and transactions with the highest risk exposure**.

Our suggestion is consistent with the risk-based approach, which provides that mitigation measures applied to payment instruments for enhancing their security shall not impair operational capacities of financial institutions' systems.

It is worth mentioning that the financial industry and payment schemes have set up systems and procedures to enable high standard of security and transparency of secure electronic payment flows made with any account-based payment instruments – including *ex ante* and *ex-post* controls (frauds detection, sanction screening, etc.). Those secured payment instruments that form a vast majority of electronic transfers (+95%). As opposed to abovementioned payment means, prepaid/bearer payment instruments present a much higher level of ML-FT and fraud risks (because their features include anonymity and charging by other untraceable means of payment). The FATF should therefore subject the benefit of the exemption to stricter conditions for prepaid/bearer instruments.

However, we note that proposes changes will require the inclusion of the card number and the name and location of the issuing and acquiring financial institution in payment messages for every card transaction.

We would like to outline that the addition of such data to accompanying transfers of funds for all card payments would necessitate huge adaptations to current processing systems of financial institutions and changes of standards and schemes currently used worldwide by the banking industry on a global scale. Indeed the instantaneous nature of payments at point of sales that requires completing the transaction in a very short time would not enable efficient checks of those data at the time of the payment transaction. In addition, name-matching controls are generally complex to implement, even more for cross-border payments. Therefore, systematic performance of such controls should lead to massive rejections and backlogs/delays. In particular, false positives generated through sanction screening will require that financial institutions reject the transactions since it will be impossible to solve the alert before completing payment transaction (payments approved within milliseconds after the initiation). Finally, the collection of this information is impossible in certain situations (i.e. contactless payments).

In addition, it is worth mentioning that most card schemes provide access to information on the name and location of the issuing and acquiring financial institutions after payment transactions are completed (generally by using the unique transaction identifier number) that can be retrieved and used by financial institutions to investigate on suspicious/risky transaction.

Option 2 could significantly increase the running costs of ATMs and the cash supply in general. This could, in particular when measured against the very limited effectiveness of the proposed requirements, decrease the economic viability of offering, and hence the access to, secure, reliable and fast cash services.

Such structural changes would therefore generate significant operational costs that cannot be justified by the little benefit they would bring from a risk mitigation perspective (as mentioned above, efficient mitigation controls and mechanisms already exist).

Given those issues, we think that:

- **it would not be relevant from a risk-based perspective to apply the proposed changes to every card payments for the purchase of goods and services at point of sales**. Other relevant solutions exist to reduce the risks, including controls performed by payment schemes operators ;
- **it would be more efficient for the fight against money laundering / financing of terrorism and fraud to restrict the use of anonymous card as prepaid card or gift card** ; and
- it would be judicious to consider alternative technical solutions, which can prevent the execution of risky or prohibited payment transactions and withdrawals ahead of the client instructions on a case-by-case basis (*e.g.* monitoring of BIN codes for cards, restrictions on withdrawals and payments for cards issued by institutions subject to restrictive measures, and the setting of specific thresholds, etc.).

- **Q.2:**

According to the risk-based approach and technology neutrality, which are key principles of AML-CFT, payment means with similar features and use cases should be treated on an equal footstep regardless the type of payment means, since their ML-FT risk profile would be similar.

Therefore, any payment transaction made through account-based payment instruments could avail of the exemption provided that the following conditions are met:

- the payment transaction is technically identified as a purchase of goods and services ;
- the payment transaction is initiated at a point of sale of merchants (e.g. payment terminals, payment interface, etc.); and
- the payment is of an instantaneous nature.

(For further details, please refer to our answer to Q.5).

The exemption should benefit to any means of payment with such features other than cards (including credit transfers).

- **Q.3:**

Subject to further technical validation on behalf of the operators of payment schemes, we suggest considering the following addition to footnote 47:

- 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. **Where, subject to the respective rules of the card network, the account numbers (e.g. BIN/PAN or acquirer BIN) allow for the**

unambiguous determination of the issuing or accepting financial institution's names and locations, the inclusion of these account numbers may suffice.

While such a "unambiguous translation" should in any case be possible for financial institutions, it is also conceivable to make it available for public authorities to support their efforts in the context of AML/CTF.

Application of the exemption to different card types

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?

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?

EACB answer:

- **Q.4:**

As **mentioned above in our answer to Q.1 to 3, we do not support the extension of the exemption to account-based payment cards (including debit and credit card).** Those instruments do not present significant difference in their ML-FT risk profile so they receive equal treatment under the R.16.

The risks highlighted by FATF may be managed and mitigated through alternative and more appropriate measures. For example, the identification of a shell bank or shell company would not be improved by the integration of information in the payment messages. If the risks raise from the payee (for example if the payee is a fake merchant), the situation could be better identified and monitored by the PSP of the payee, that is better placed to identify the risks.

More generally, the risks and vulnerabilities identified by FATF could be addressed through a reinforcement of requirements (supervision/CDD/monitoring of transactions) rather than the amendment of Rec 16, as this information is already accessible, event not included in the payment message.

However, **prepaid cards and bearer based payment instruments present a much higher vulnerability to ML-FT and fraud risks** (because their features include anonymity and charging by other untraceable means of payment). The FATF should therefore subject the benefit of the exemption to stricter conditions, and could be limited to prepaid/bearer instruments.

Accordingly, **we think that only the prepaid cards satisfying the following conditions should be eligible for the exemption**:

- The prepaid cardholder is subject to a KYC equivalent to the one carried out at the opening of a bank account;
- The cards are associated to an account of the cardholders opened within the books of the issuing institution (therefore, anonymous features should be prohibited or subject to stringent conditions, including the demonstration that it is impossible to obtain information on the cardholder or issuer) is similar to the one used for debit/credit cards ; and
- The card are charged exclusively with funds registered in the cardholder account.

- **Q.5:**

We do not agree with the FATF statement asserting that "it is not appropriate to extend the card exemption to other payment means (*e.g.* instant payments) (…) due to different nature of the associated risks with other payment means".

Please refer to our answer to Q.2 above: any payment transaction made through account-based payment, regardless of the type of instrument, should benefit from the exemption provided they have common features that confer to them equivalent ML-FT risk profile.

For instance, as regard **payment transfers (notably instant payment)** initiated for the purchase of goods and services, we note that:

- both payment transfers and cards may be use in relation to the same underlying activities between the parties to the payment transaction / performance of contractual payment obligations;
- transaction initiated through both means of payment will be processed first through the merchant's payment acceptance system;
- both means of payment are subject to similar constraints in term of speed of transaction that make impossible the performance of controls / analysis once a transaction is initiated at the point of sale (controls and screening are performed ahead of the initiation of transactions); and
- since payment transfers and cards are account-based payment instruments and as such, their use is subject to similar initial and ongoing client due diligence procedures.

It follows from the above that card payments (providing the card is associated to a payment account opened within the books of the issuer) present a similar AML-CFT risk profile as payment transfers/instant payments, with common processing systems and mitigation techniques.

Therefore, the exemption for the purchase of goods and services should also concern those means of payment.

Scope of "withdrawal or purchase of cash or a cash equivalent"

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

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?

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?

EACB answer:

- **Q.6 and Q.6bis:**

We do not support the application of recommendation 16 to cash withdrawals and purchase of cash or cash equivalent for reasons set out above in our answer to Q.1.

We believe that these situations should continue to benefit from the exemption. Indeed:

- where domestic cash withdrawals are requested by customers at ATMs of the institution that operates their account and issued the card associated to that account, because the information on the acquiring bank will not be relevant and the mention of the issuing bank is inoperative because it debits the account of the card-issuing bank;
- applying the R.16 to all cash withdrawals would not indeed bring significant improvement in the transparency and security of these transactions. Given the instantaneous nature of cash withdrawals, financial institution have set up technical solutions to flag potential risky withdrawals ahead of the client instructions, and AML-CFT controls are also performed a posteriori as part of financial institution's transaction monitoring system; and
- finally, the implementation of additional transparency requirement provided under the R.16 for cross-border or domestic cash withdrawals above €1000 could be technically difficult to implement in internal systems for the operation of ATMs. Therefore, there is a risk that such withdrawals would be made unavailable through ATMs and then would have to be made exclusively at bank counters.

Considering the above, revision of the R.16 shall also take into account the fact that for cash withdrawals, only the card issuer would have the capabilities to control the accuracy of payment information and the lack of frauds (*i.e.* not the institution or undertaking operating the ATM).

As regard the treatment of credit, debit and prepaid card, we are of the opinion that prepaid cards should be subject to stricter scrutiny because of their ML-FT risk profile being higher. Please refer to our answer to Q1. Option 1 and Q4.

As stated above, we strongly believe that R16 should not be utilized to reduce financial crime risks in the space of cash and cash withdrawals, but rather outside of R16 (i.e. through CDD measures).

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

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?*

EACB answer:

- **Q.8:**

The established rules pursuant to the existing paragraph 7 have proven to strike the right balance between supporting the fight against financial crime and allowing for a smooth operation of cross-border payments. Therefore, we believe that a structural amendment is not necessary and could indeed be counterproductive, as we fear that this could result in a significantly slower processing of cross-border payments due to the amount of data that requires collection by financial institutions or customers. What is more, we want to raise the attention to a possible heightened risk in view of sensitive customer/personal data theft and leaks in case the regulatory provisions prescribe the transmission of Personal Identifiable Information (such as date and place of birth of a natural person, address). We also would like to draw the attention to the fact that the information on the Creditor requested is unverified information directly received from the payer.

Notwithstanding the above, carefully extending the set of originator and beneficiary information in the case of legal entities could, however, be beneficial. We therefore support the general idea of including the LEI/BIC/unique official identifier as best practice and encourage Payment market infrastructures (PMIs) to provide supportive data structures by e.g. migrating to ISO20022 (please note also our related considerations in view of effort and implementation period under question 17).

However, EACB members expect that the possibility to include at least one of three information element (*i.e.* address, town or country) may create inconsistencies in payment standards applied by banks involved in international cross-border payment transactions (e.g. the country of incorporation of the originator's bank would not require the same information element than the country of incorporation of the beneficiary's). We do not see how a bank (or even the originator) in country A knows what options are available in country B. We think that as a first step it would be much helpful to clarify what is meant with an "address". We would also greatly appreciate you could provide explanations as to what a standard address consists of. We only have learned it can be replaced by a town name and country.

Referring to both options 1 and 2, mandating the address (para 7(c)) and, where applicable, the LEI/BIC/unique official identifier (para 7(e)) of the beneficiary could cause severe disruptions since this presupposes that the originator is always capable of providing these information to the originator's bank (the originator's bank cannot possess these information by itself). We strongly recommend limiting the mandatory character of these information to the originator, whereas it could become optional (or recommended) for the beneficiary. With a view on option 2, the same applies to the suggested national ID number or unique official identifier of the beneficiary where she/he is a natural person.

If the FATF decides in favour of a mandatory inclusion of extended beneficiary information, the particular situation of euro denominated SEPA payments into countries outside the European Economic Area (EEA) should be taken into account, e.g. to the United Kingdom or to Switzerland: A country can become part of the Single Euro Payments Area (SEPA), if it satisfies certain legal requirements measured against the respective EU standard. As a result, the originator faces the same efficient technical provisions as regards the payment order than for a SEPA payment to an EEA country – a credit transfer in euro to Switzerland feels the same as a payment to France. This customer-friendly and regulatorily justified simplification should not be put in doubt by extended data requirements aimed at "actual" international payments.

Additionally, member banks are concerned about the **inclusion of beneficiaries' supplementary identification information** (*i.e*. available identifier code/number; place and date of birth for natural persons). Indeed, from a French personal data protection perspective, the French data protection authority may be reluctant to authorize the processing of data of payment parties being natural persons, even more in the lack of a business relationship with the institution processing their data (since data would be treated without the consent of the data subject).

It follows that **Option 2** – complete alignment in information elements for the originator and beneficiary, including the fill-in of supplementary identification information about the beneficiaries who are natural persons – would not be easily implemented.

Furthermore, as regard **other identification information to improve the reliable identification of the originator and beneficiary**, we would not fully support the requirement for financial institutions to collect and communicate the national identity number, or a unique official identifier, or the customer identification number, since it would be redundant and not provide much benefit in term of reliability. For instance, requesting the customer identification number would not add a distinct information from customer's bank account number (since the

identification number may be a part of the account number / IBAN).

Finally, we suggest adding a clarification to footnote 48 implying that the account number may be used as the originator's customer identification number (para 7 (d)) subject to it fulfilling the said requirements.

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

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?

EACB answer:

- **Q.9:**

We favourably welcome the suggested approach since it corresponds with the IBAN definition pursuant to the ISO 13616 standard and the resulting broadly applied business practice. We think that matching the country code of the IBAN with the location of the account will facilitate the fight against money laundering and terrorist financing.

However, please be mindful that to achieve this principle across all jurisdictions, countries that might currently deviate from this standard would require a multi-year "change" project effecting all parties in the payment chain.

Nevertheless, we would suggest to use the name 'account number' instead of IBAN (an IBAN is also an account number) because globally, countries does not always use an IBAN.. ISO country codes also occur in non-IBANs. A virtual account number never contains a balance but is a reference to a 'real' account number. That link must be recorded somewhere (not just in the bank's administration of the account number). Moreover, it is essential to that the country code and account number structure to always match (will also be a requirement of the linking bank).

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

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

EACB answer:

- **Q.10:**

The EACB calls for more guidance on this specific revision of R.16, as we believe that the current drafting lacks clarity, therefore creating legal uncertainty for financial institutions.

Additionally, the underlying issue (fraud in the context of payments) does not perfectly correlate with the purpose of the FATF Recommendation 16. We warn against blending different policy goals extraneous to each other since this runs risk of undermining their overall effectiveness.

We agree that imposing to the beneficiary's payment services provider to verify that the information in the payment message matches the information it has on the beneficiary on a risk-based approach could contribute to combatting frauds and financial crime.

Nevertheless, we see several content-related issues in this new requirement. The problem is mainly the definition of the beneficiary. Who is the real beneficiary? The term 'intended recipient of the money' appears to be inadequate because lawyers are of the view that the beneficiary is the party to whom payment is validly made. In case this corresponds to an (intermediary) payment institution, then that is the intended beneficiary. We therefore believe that a description would be very useful. For the EACB, any 'payment institution' should not be referred to as a client or beneficiary unless it is acting on its own behalf. Furthermore, we would like to state that it is important to keep in mind that it will be very costly to ask banks to check the beneficiary in the payment instruction with the client who should be credited. Which percentage will be sufficient to process the payment?

We would also like to emphasize that the **current drafting of this proposal would raise serious technical concerns**. Currently we are not aware of tools permitting financial institutions to compare payment information with client information input and updated in internal databases for all payments. We expect that creating and implementing such tools would require significant time and resources. In addition, depending on the degree of information to match together and significant volume of payment flows, this would generate massive false positives and rejects, the majority of which would affect clients with no/low financial security risks.

Considering the above, we think that the drafting needs revision, in order to give more leeway to financial institution for detecting payment transactions potentially affected by frauds on a risk-based basis. Financial institutions have actually set up / considered external fraud prevention measures and tools to secure payments, which include *ex ante* controls and listings (*e.g.* internal listings of IBANs identified as involved in frauds; listing of banks known for poor internal arrangements fraud prevention through investigations and public sanctions of authorities; alerting systems flagging activity sectors most exposed to frauds, etc.).

f. Definition of payment chain (paragraph 23)

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?

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?

EACB answer:

- **Q.11 and Q.12:**

One observation we want to highlight, before setting out our thoughts with respect to the preferred Option 1, is that for instance Money or Value Transfer Service (MVTS) increasingly structure payments into multiple legs as depicted under f., but in most cases and different to f., the MVTS in Jurisdiction L and N are either the same legal entity or related parties.

We agree with Option 1 that the information needs to be transferred from the start (i.e. payment initiation) until the payment is executed in full. This includes the information of the debtor, debtor agent, creditor agent and creditor. **We notably believe that it is fundamental that the real originator and the real beneficiary are included in the definition**. Indeed, a payment chain always starts with an instruction to the bank of originator and it will end when the intended beneficiary will receive the amount on his account with his bank. All other banks and MVTSs are payment processors and should never be mentioned in the fields that indicate originator/beneficiary. Option 1 will not solve the issue as it still result in a split (a pay in to the MVTS and a pay out from the MVTS to the merchant).

In the example of payment structure showed in the Explanatory Memorandum, we consider that the payment chain should start with the MVTS/ third-party payment service provider (with whom the customer doesn't hold an account). In this case, all the required information would have to be transmitted in the payment chain by the MTVS receiving the instructions.

The recommendation.16 should then formalize the MVTS provider's exclusive responsibility for carrying out the sender's customer due diligence (CDD).

We therefore suggest:

1. limiting the role of the payer's account bank to sending the funds, without having to receive or control information on the payment transaction that was initiated by the payer through a MVTS/ third-party payment service provider; and
2. in any event, the account bank that will transfer funds following the initial payment instruction should not be held liable with respect to any incorrect or false information concerning the underlying transaction collected and disseminated under the responsibility of the MTVS.

We also recognise the legitimate use of net settlements to transfer liquidity intra- and inter-company across jurisdictions and currencies to enable effective and efficient payment execution. While the PMI in Jurisdiction N might be the first and last leg used for the execution of the Payment Instruction received from Client X in Jurisdiction L, the description under Option 1 is rightly reflecting this where the MVTS must select a PMI supporting cross-border payments and provide full and accurate disclose of relevant parties and agents.

As part of option 1, paragraph 23 should also give guidance on the possible courses of action where the (account holding) financial institution of the originator detects missing required information. This guidance should give sufficient leeway to cater for the diverse nature of underlying business agreements and national regulatory provisions. We propose the following extension to paragraph 23:

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. **Where the financial institution that holds the account of the originator identifies a lack of required originator information or required beneficiary information, it may, depending on the underlying business agreements and further regulatory provisions, either request the originator or the financial institution that has received the transfer instruction from the originator to provide the necessary information.**

In order to safeguard a clear understanding and avoid any abuse in the chain, we recommend reminding PMIs to clearly document and publish the payments in scope of the related clearing system in their rulebooks. Further, PMIs must take responsibility to ensure the payment messaging standards used 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.

Option 2 suggests merging two independent actions into a single payment transaction. This results in a complexity neither supported by any payment messaging standard nor PMI. We must be mindful not to discriminate the MVTS from a traditional FI where the funding of an account (own transfer across two banks) would be considered a separate transaction from any (future) payment instruction(s). Key for us and echoing FATF's own's principle: 'same activity, same risk, same rules'.

We fear that Option 2 could inadvertently disrupt legitimate business models of new service providers (PSPs), as a result and contrary to the G20 goal, it may raise the costs of cross-border payments, and even undermine the G20 objective of inclusion. To avoid these negative consequences, we recommend FATF to request PMIs which allow cross-border payments to be settled via their clearing infrastructures to enable the provision of all parties and agents by introducing ISO20022. At the same time encourage national competent authorities to ensure that only these domestic clearing systems that are capable of transmitting all relevant information and to enforce the usage of the appropriate data fields.

g. Conditions for net settlement (paragraph 24)

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?

EACB answer:

Q.13:

Option 1 is not a good option as a payment never starts at a bank unless the payment is made on his own behalf. The end-point should always be the intended beneficiary and not his bank or a MVTS. The explanatory pictures are more clear than this text. Please add the second picture.

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

EACB answer:

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?

Q.14:

As Recommendation 16 is the only rule making recommendation regarding the data quality of the originator and beneficiary, it is key to make sure that the requirements are very clear, otherwise it would only make this exercise costly for stakeholders.

We strongly acknowledge the merits of R.16 as it provides an internationally harmonised standard for the inclusion of originator and beneficiary information in cross-border payment flows. It is only logical that the FATF validates its adequacy at the background of developments in the technological, business and AFC spheres.

By the same token, we caution against "overloading" data transmission requirements where these follow to burdens for originators, particularly for consumers. It is the stated goal of policy makers and the financial services industry to make payments more accessible and inclusive. Additional data requirements can have a severe counterproductive effect in this respect and need to be carefully weighed against their actual benefits (for specific examples see answers to Q.1 and Q.8).

i. Impact on other FATF Recommendations:

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.

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

EACB answer:

Q15-16:

We would recommend that the definition of a MVTS include not only Money Transfer Organisations (MTOs) but also Payment Institutions.

Additionally, following the principle of 'same activity, same risk, same rules', a perspective inclusion of the VA sector in the scope of R.16 is to be welcomed. This is underlined not least by the corresponding FATF's expectation as laid down in paragraph 7 of INR.15.

Within the European Union, the revised Transfers of Funds Regulation (Regulation (EU)

2023/1113 - TFR), which transposes the R.16 provisions into Union law, has already included crypto-assets within its scope. Preparatory efforts to ensure implementation of and compliance with the legal provisions reflect the resulting challenges for IT systems and business processes. These challenges include, but are not limited to, the following points:

• In contrast to the established fiat payment ecosystem (SWIFT, ISO20022), there is no single standard for the transmission of crypto-transaction related information, which can make the submission of structured information with the payment flow difficult.

• In contrast to the fiat-world, person-to-person transactions could take place (using a risk-based approach) from a hosted wallet (person A holds wallet with Financial Institution 1) to an unhosted wallet (person B), or vice versa. Here, the submission of the required information may not be ensured.

• The concept of domestic vs international transactions may not be applied as easily as for fiat movements.

It should be emphasized that, in particular, crypto-assets that are treated as financial instruments under existing Union capital market law do not fall within the scope of the TFR (cf Art. 3(14) TFR). This approach of separation from conventional capital market law should be maintained in connection with crypto-assets. As has been the case to date with the regulatory treatment by way of a technology-neutral approach, it should make no difference to the FATF's recommendations on which infrastructure these financial instruments are issued. We recommend that FATF closely monitors the developments in the European Union and seeks close collaboration with the European Banking Authority and local industry representatives to leverage on their expertise and ensure a globally harmonised approach, respectively.

The category "Payment(s) or value transfers" should be defined more precisely to avoid possible misinterpretations arising from the broad term "value". We assume that the term "value transfer" will continue to be understood as transactions in connection with e.g. remittance payments and is not to be applied in the context of capital markets or other asset transactions. We suggest the following amendment:

Payment**~~s(s) or value transfer~~**:

refers to any transaction carried out on behalf of an originator through an ordering financial institution **or Money or Value Transfer Service (MVTS)** by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same.

In addition, we suggest aligning the "Cover Payment" definition with the definition used by SWIFT in order to facilitate a uniform understanding ("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.").

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

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?

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?

EACB answer:

Q17:

In consideration of the possible changes outlined in the consultation document and the necessary technical adjustments and communication measures for customers, **we currently expect an adequate implementation period to be at least 36 months after the transposition into the respective national law.**

From a global perspective, the FATF should acknowledge that a variety of the proposed changes presuppose the technical capabilities made possible by the ongoing global migration to ISO20022 payment messages. Payment market infrastructures (PMIs) in many major economies, such as the Euro area, have already successfully managed this migration or are well on track to achieve it in the foreseeable future. However, in cases where economies face severe delays in their migration efforts, the technical prerequisites for complying with new regulatory requirements could soon be called into question – with potential international repercussions in the case of global payment chains stretching across multiple PMIs. **Therefore, we recommend that the FATF seeks a close dialogue with jurisdictions and PMIs which are not yet "ISO20022-ready" to identify possible bottlenecks and gain a better understanding of realistic lead times.**

Notwithstanding these considerations, any significant changes to the provisions for ATM cash withdrawals or card payment networks might need a significantly longer implementation period.