



BNP PARIBAS

16, boulevard des Italiens
75009 Paris

Paris May 3, 2024

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

RE: Comments of BNP Paribas on the proposed revisions to R.16/INR.16

Dear Ms. Clerc,

The BNP Paribas 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 project to update R.16 to ensure its adequacy with the current payment system by taking into account the emergence of new actors, regulated or not.

BNP Paribas is aligned with the objectives of the G20's Roadmap for enhancing Cross Border payments aiming to make cross-border payments faster, cheaper, more transparent, and more inclusive and remain fully committed to the fight against money laundering, terrorist and proliferation financing.

In this field, we consider that payment transparency is key to ensure that international payment systems are not misused. For that, it is essential that the ordering payment service provider (PSP) be responsible for identifying the debtor and the creditor of a funds payment and for structuring that information in the payment message. Responsibilities of each PSP participating to the payment chain should be clearly defined.

The adding of information on the names and locations of the issuing and acquiring PSPs for transactions carried out using a card for the payment of goods or services from merchants does not seem relevant. Similarly, if information accompanying all qualifying payments or value transfers should be mandatory for names, accounts numbers and addresses of the originator and the beneficiary, further information should remain optional and be provided upon request when investigations are performed. These additions would generate considerable developments and monitoring and won't really tackle the risks highlighted by the FATF. We do not see how the beneficiary financial institution could check the alignment between the beneficiary information in the payment message, provided by the originating customer, and the verified information of the beneficiary account holder. A better way to identify fraud cases would be for the ordering financial institution to check the name and the account number of the

beneficiary before processing to the payment and ideally at an earlier stage when the client adds a new beneficiary to its' beneficiaries' list. In parallel to the transparency and the monitoring of transactions, customer due diligences of payment services providers remain key.

We also would wish to draw your attention on three specific points:

- The extension of the exception given to cards for the payments of goods and services from merchants should be enlarged to other means of payment with the same usage and the same characteristics (see Q.2),
- A clear distinction should be made between debit/credit cards and prepaid cards which present features of anonymity that should be strictly framed notably for the funding transaction (see Q.4).
- R-transactions should be exempted from Payment Transparency controls (See Q.18).

We thank you in advance of your consideration on our feedback and remain at your disposal should any clarification be necessary.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'Anne-Catherine Colleau', with a horizontal line underneath.

Anne-Catherine Colleau
Head of Group Financial Security
BNP Paribas SA

Consultation for the card exemption.

Question 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?

Option 1 clarifies that only transfers that flow from a transaction carried out using a card for the purchase of goods and services from merchants are exempted from the requirements under R.16. This option also requires that the card number and the name and location from the issuing and acquiring financial institutions' accompany the transfer.

We support the proposal to limit the exemption to the purchase of goods and services from merchants which does not raise technical issues as the nature of the payment can be easily identified. We agree that this proposal will ensure that only the purchase of goods and services are included, excluding person-to-person transactions,

However we consider that:

- The exemption scope should not be limited to card transactions. As of today, there is no difference between a card payment initiated by the merchant system (physically or online) and other typologies of instant payments initiated by the merchant system (physically or online) (see Q2),
- A clear distinction should be made between debit/credit cards and prepaid cards which present features of anonymity that should be strictly framed notably for the funding of transaction (see Q4).

Furthermore, the adding of the names and locations of the issuing and acquiring financial institutions does not seem relevant for us as:

- The monitoring of such information will be impossible during the process of the payment given the very short timeframe of the operation (whether on-line or physically like for instance the payment of a restaurant bill). Should the filtering against sanctions lists triggers a hit, financial institutions (FIs) won't be able to investigate the alert and will have no choice but refusing the payment. The issue is the same as for cash withdrawals for which we give further details below in option 2.
- From an AML point of view, we note that the majority of the risks mentioned in the memorandum is supposed to be covered by the due diligences of both the issuing bank ("use of shell companies, use of stolen credit card numbers") and the acquiring bank ("purchase of illicit goods, tax evasion"). These names and locations can also easily be obtained from the card schemes after the payment, during the classical ex-post AML/CFT investigation process.

Option 2 proposes that a cross-border withdrawal or a purchase of cash or cash equivalent, as well as a domestic withdrawal or a purchase of cash or cash equivalent with a value of 1'000 USD/EUR, be subject to R.16 requirements.

Removing a withdrawal or a purchase of cash or cash equivalent from the exemption would create the necessity to add information in the instruction process and consequently, this information would have to be checked against national sanctions lists by the ATMs operators. In case of a match between the name of the card holder and a listed name, the timeframe for authorizing the withdrawal or the purchase of cash or cash equivalent does not allow for the analysis and decision whether it is a "true"

or a “false” hit (no possibility to contact the cardholder to collect and check the information and documentation related to the withdrawal or purchase of cash or cash equivalent).

The only possibility would be to refuse any withdrawal or purchase of cash or cash equivalent triggering a “hit” against a list. This would create a strong discrimination situation, preventing people concerned by “homonymy” (name and/or first name) to perform a withdrawal - or purchase of cash or a cash equivalent. The impact would be disproportionate and would raise a financial inclusion issue.

Withdrawals or purchases of cash or cash equivalent are already subject to limitations (thresholds) and card issuers are responsible for the ongoing screening of their cardholders’ names against sanctions lists as well as for monitoring the activities of their clients. Therefore, we advocate for a better implementation of FATF standards across the jurisdictions rather than duplicating control tasks through a filtering requirement that would be extremely complex to be put in place or investigated by the counterpart financial institution.

Question 2. Are 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?

We recommend considering the key principle “same business, same risks and same regulation” and to apply a consistent approach, irrespective of differences in the means of payment used. The exemption to R.16 requirements should be driven by “usage” and not by the nature of payment mean.

Consequently, we are on the opinion that the exemption should be extended to all payment means corresponding to the same usage and with the same characteristics e.g.:

- Identified as “goods/services payments” as part of information that accompany the transfer (*Example: a dedicated code/reference in the payment message field*),
- Processed in a short timeframe to authorize/approve/validate the transaction due to instantaneous operation design,
- Initiated by the merchant payment system (payment terminal, payment page...).

The exemption must therefore encompass, cards, QR codes followed by instant wire transfers – like SCT inst – and similar payment means provided that they meet the above “usage” and “characteristics” requirements. This will permit to *i)* maintain the same level playing field, *ii)* avoid unfair competition, *iii)* avoid discrimination against end-user based on their names/origin, *iv)* maintain financial inclusion goal and strategy.

We would like to remind that the purchase of goods and services usage responds to economical needs and a significant part of these needs require a certain level of “instantaneity”. Any payment mean’s limitation, whatever the reason (reject, timeout...), will induce the buyer to use another payment mean (competition issue) or to use cash (increased AML risks and less inclusion).

Question 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?

PSPs do not have the capability to populate the names and the locations of the issuing and the acquiring financial institutions without a common “worldwide” database containing names, locations, and associated codes. The deployment of that kind of database can only be made at card schemes level and the development and update of the information would induce significant costs.

Furthermore, some significant developments would also have to be done to both add the information in the payment chain and take the information into account in the acquiring systems on a worldwide basis.

Costs would not be reasonable compared to the impacts/benefits of the measure that will not improve financial crime detection. In any case, controls can only be made after the transaction due to “instantaneous operation design” and the related information can already be obtained after the transactions as part of the investigation.

Application of the exemption to different card types

Question 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/CTF 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?

The FATF proposal is that cards should be included in the exemption whatever their nature (ie. credit, debit and prepaid) provided that they meet both “usage” and “characteristics”.

However, we consider that a particular attention should be paid to prepaid card subject to anonymity and/or that could be funded by a channel that do not allow the identification of the creditor (cash, prepaid “coupon”, SMS messages...). We note that most National Risk Assessments consider prepaid cards with these characteristics as highly sensitive from an AML/CTF standpoint. They can be used by money launderer, notably via mules.

If the exemption on withdrawals and purchases of cash or cash equivalent remains (e.g controls can only be made after the transaction due to “instantaneous operation design”), we advocate for the reinforcement of the AML/CTF framework on prepaid cards with the following measures:

- Delivery of prepaid cards should be limited to specific use cases (close loop networks and thresholds based);
- Cardholder due diligence measures should be equivalent to those requested for opening a bank account,
- The source of funding of the prepaid card should be limited to the account of the card holder. Cash or funding from a third person account should be prohibited.
- Controls on the funding transaction should be strengthened (rather than the use of card).

Question 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?

We are of the opinion that the exemption granted to cards should be extended to all payment means corresponding to the same usage and with the same characteristics. See Q2 answer.

It is important to highlight that some territories (like the European Union) did not choose to develop card schemes and have started to develop (and invest in) instant payment schemes based on wire transfers. Some solutions like the European Payment Initiative are being deployed to compete with foreign card schemes (Visa, Mastercard...) notably for goods/services payments.

The EU regulator – taking into account proportionality impact, inclusion issue and technical feasibility has introduced an Article 5d in the Regulation (EU) No 260/886 of the European Parliament and of the Council amending Regulations (EU) No 260/2012 and (EU) 2021/1230 as regards instant credit transfers in euro: "*During the execution of an instant credit transfer, the payer's PSP and the payee's PSP involved in the execution of that instant credit transfer shall not verify whether the payer or the payee whose payment accounts are used for the execution of that instant credit transfer are persons or entities subject to targeted financial restrictive measures [...]*".

Limiting the exemption to "cards" would generate unfair competition for other instant payment solutions and create uncertainty for various stakeholders. This is a strong level playing field issue that could potentially lead to various actions in front of competition authorities, should regulations based on such FATF proposal being adopted.

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

Question 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?

Cash withdrawals and purchase of cash or cash equivalent should remain within the exemption of R. 16. See Q1 answer option 2 and whatever the nature of cards.

We are of the opinion that removing withdrawals and purchases of cash or cash equivalent from the R.16 exemption would hamper access of customers to their accounts and own funds, be perceived as a threat to the basic right of consumers and undermine confidence in banks.

Question 6. bis. 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?

See Q1 option 2 and Q2 answers.

A better approach would be for National Authorities to limit/restrict cash withdrawals from financial institutions targeted by sanctions measures through the monitoring of technical references - like BIN codes for cards –and/or to define a risk-based approach (thresholds, authorized distribution network, ...).

Question 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?

We agree that cash equivalent should be better defined or clarified in the future FATF guidance.

We would however recommend excluding any payment via securities from the scope.

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

Question 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?

In order to improve the reliable identification of the originator and beneficiary and increase efficiency, paragraph 7 sets out updated requirements for the specific information that should be included in the payment messages. Option 2 proposes the full alignment of the information required on the originator and the beneficiary.

The beneficiary information included in Option 2 would induce technical developments and the set-up of new controls. This information would be provided by the originator on a declarative basis. One can fear that this solution would generate numerous hits and consequently burden and costs without giving significant added value.

Consequently, we support the option 1.

However, if we agree that a) the full names of the originator and the beneficiary, b) the account numbers of the originator and beneficiary (where such account is used for the transaction) and c) the address of the originator and the beneficiary (if country and town are sufficient) are necessary to better identify them and to be more efficient, we consider that the other requirements d) and e) should not be included in the message but provided when requested by the counterparty as part of their investigation.

Filtering and screening are done based on the account number, the name of the customer, the town and the country where he lives. Should further investigation be needed, additional information (especially date and place of birth) has to be provided by the originator bank upon request.

Information like national identity number or customer identification number aren't of any utility for banks investigations. The address is absolutely necessary and, in this regard, the country and the town name are sufficient.

Addressing transparency in case of virtual Iban and other similar account naming conventions (paragraph 7(b))

Question 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?

We consider that a Virtual IBAN ("VIBAN") presenting a country code different from the customers' master account country goes against the payment transparency principles upon which "countries should have the ability to trace all wire transfers" and "the full traceability of transfers of funds".

Indeed, allowing a financial institution to provide a customer with a VIBAN referring to one country when the customer's master account is in another country is a way to disguise a cross-border payment into an undue domestic payment. VIBAN should not be used to lighten obligations on payment transparency by hiding cross-border transactions as domestic transactions that are not subject to the same obligations.

It is important to remind that financial institutions are not able to differentiate a VIBAN from an IBAN (both have the same characteristics) and that currently technical standards of the schemes do not allow the adding of the "customer account location". Hence, one should leverage on the "reference account" characteristic to introduce requirement for the VIBANs to always identify the master physical account. As an example, a French master account – related VIBAN should have a FR code and a French IBAN structure. This would prevent the use of a foreign VIBAN structure.

Moreover, we would like to bring FATF attention on transactions from PSPs collecting funds for a Merchant identified by a VIBAN.

Currently the completion of the beneficiary and ultimate beneficiary fields in the VIBANs is optional and barely done. This does not allow other financial institutions participating to the payment flow to get the necessary information for meeting their AML/CFT obligations. Therefore, we suggest making compulsory the completion of these fields e.g.:

- Name of the PSP in the field dedicated to the beneficiary's name,
- Name of the client of the PSP in the ultimate beneficiary's dedicated field.

Obligations on beneficiary financial institutions to check alignment of beneficiary information in payment messages

Question 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?

The proposal is for the beneficiary financial institution to check the alignment between the beneficiary information in the payment message provided by the originating customer, and the verified information of the beneficiary account holder. This question has to be reviewed taking into account comments already provided in question 8 above (provision of information on a declarative basis).

Although we support the objective of better addressing fraud risks, we consider that the proposed alignment raises critical unintended consequences.

Financial institutions cannot automate such control without adding a fuzzy matching check between the information declared in the payment and the information contained in the KYC data base. And even with the addition of a “fuzzy matching” layer, a high volume of discrepancies would remain (for example different way of spelling a same individual or entity name –e.g. BNP Paribas / Banque Nationale de Paris Paribas SA / BNPP).

It is also important to consider that all names contained in the KYC database are not necessarily required and populated as such in a payment message (example: Jesus Hernandez vs Juan Maria Jesus, Lopez Hernandez). A massive rejection of transactions has to be expected with the current alignment proposal.

We would also like to underline some current identified behaviors with domestic transactions where the Originator is populating the beneficiary’s name with terms such as “MUM” or “DAD” “my account in bank XXX”... which would systematically generate alerts should alignment be requested. Beneficiary’s name is not a regulatory request for domestic transactions and it is unclear in the proposal if such controls should be (if validated) implemented only for cross-border flows or also for domestic transactions.

In addition, the purpose of the controls is unclear: what is expected from the beneficiary institution when a discrepancy is identified in relation with a client? The beneficiary institution has already access to its client KYC documentation and should rely on it instead of considering declarative information contained in the payment message. An information provided by an unverified party (i.e., the Originator) should not trigger a KYC review or additional action plans on KYC database.

However, we recommend, from a fraud perspective standpoint, that controls should be performed at initiation by the originating Bank, during the validation step of the addition/creation of a new beneficiary.

Definition of payment chain (paragraph 23)

Question 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?

MVTS providers are increasingly collecting and disbursing funds through electronic means and often the MVTS or other service providers send wire transfers to other financial institutions without specifying the name of the true originator.

We support option 1 of paragraph 23 whereby the payment chain starts at the financial institution that receives the instructions from the originator and ends at the financial institution that services the account of the beneficiary or remits cash to the beneficiary.

In the described first scheme, the only actor that has access to the entire “end to end” information is the MVTS. The MVTS should therefore be liable for providing the necessary information – especially ultimate beneficiary information – to other financial institutions. A financial institution involved in a transfer should not be held liable beyond that transfer.

In the first leg, the financial message is initiated by the Payer (customer of the MVTS), however the transaction is a funding operation that could cover several payments. It is therefore impossible for the originator bank to know if there is one or several ultimate beneficiaries.

In the second leg, the transaction is a balance account adjustment operation between MVTS accounts held in different banks. This payment can cover hundreds of different underlying payments for different ultimate’s parties.

Last leg: the beneficiary bank cannot know that she should expect information on an additional ultimate originator in the payment message.

All the ultimate parties (ultimate originator / ultimate beneficiary) should be identified in a dedicated field in each transaction in the payment chain as soon as it is the same transaction (same purpose, same amount and same timeframe).

The above scheme description permits to highlight that only MVTS can provide necessary information. He should also populate the information in the dedicated payment message fields according to the case (ultimate originator, ultimate beneficiary...).

Question 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?

We support the idea of adding the account number and financial institution’s name which is the origin of the funds in case where the origin of the funds is a financial institution other than the ordering financial institution (footnote 2). All the actors in the payment chain should be identified in a dedicated field in each transaction as soon as it is the same transaction.

However, it is important to clarify in R.16 paragraph 23 that the “instruction” refers to the payment instruction of the MVST to the beneficiary and not to the funding instruction (the MVTS has already collected the funds from the Payer’s Bank).

Conditions for net settlement (paragraph 24)

Question 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?

No additional risks to be addressed.

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

Question 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?

We want to reiterate the importance of enlarging the exemption to R.16 requirements (see Q1 and Q2 for more details).

We see significant risks of having a large number of people being excluded from the possibility to purchase goods/services and/or to perform cash withdrawals due to their name/origin should the recommendation exemption not be enlarged to other means of payments than cards.

Impact on other FATF Recommendations

Question 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.

No specific view on this point.

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

The previous definition of beneficiary Financial Institution was providing more clarity. It should not be limited to the remits of cash and we suggest the following definition: “The beneficiary financial institution is the end point in a payment chain which makes the funds available to the beneficiary”.

Impact of implementation of R.16/INR.16 revisions

Question 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?

The timeline should take into account the need to reduce/limit potential discrimination impacts, to protect competition and to maintain proper financial inclusion strategy. The timeline can include several steps.

Question 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?

We would like to bring to the attention of the FATF the payment transparency issue that remains with “R-transactions” (reject/return/refund).

We suggest clarifying that R-transactions are exempted from Payment Transparency controls even when rejected for compliance reason(s) for the following reasons:

- These flows have already been subject to payment transparency controls by the Ordering PSP, the IPSP(s) and the beneficiary PSP.
- Different Market practices exist on the topic as some PSPs tend to consider a R-transaction as a Bank-to-Bank transaction (equivalent to MT202 and not to MT103/MT202COV), the funds being retransferred to the bank and not directly sent to the client.
- There are cases where flows are rejected due to a lack of mandatory information but where the counterparty does not accept the R-transaction (e.g. the off-boarding of the client of the counterparty occurred between the initial transaction and the R-transaction).