Brussels, 26 February 2024
RV

EACB answer to the EBA consultation on the Guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under Regulation (EU) 2023/1113 (The 'Travel Rule' Guidelines)

February 2024

The **European Association of Co-operative Banks** (EACB) is the voice of cooperative banks in Europe. It represents, promotes, and defends the common interests of its 27 member institutions in banking as well as cooperative legislation. With 2,500 banks and 36,500 branches, cooperative banks are widely established across the European Union and play a vital role in its financial and economic system. They have a longstanding tradition serving their 225 million customers, mainly consumers, retailers, and communities. An important task of the EACB is to raise awareness on the unique characteristics of the cooperative business model: democracy, transparency, and proximity. In Europe, cooperative banks represent 89 million members, providing employment to 712,000 individuals and maintaining an average market share of approximately 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 appreciates the opportunity to provide comments on the EBA draft Guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes.

We welcome the additions presented by the European Banking Authority under these draft guidelines. Nevertheless, in order to establish a more logical and practical framework under the Transfer of Funds Regulation, we suggest incorporating specific modifications and clarifications into the guidelines.

EACB answers to the questionnaire

Question 1: Question 1. Do you agree with the proposed provisions? If you do not agree, please ex plain how you think these provisions should be amended, and set out why they should be amended. Please provide evidence of the impact these pro visions would have if they were maintained as drafted'?

2. Exclusion from the scope of Regulation (EU) 2023/1113 and derogations

2.1. Determining whether a card, instrument or device is used exclusively for the payment of goods or services(Article 2(3) point (a) and (5) point (b) of Regulation (EU) 2023/1113)

Paragraph 4.

EBA specifications on measures and actions to be taken to benefit from the exclusion of card payment exclusively used for the purchase of goods and services are useful.

However, considering the different organizations of the institutions involved, we believe that it would be more appropriate to formulate these recommendations as best practices rather than binding guidelines (suggested by the use of the word "should"). Indeed, best practices would allow each institution to decide to implement these measures efficiently and adapted to their compliance organizations. We support a more flexible approach, all while preserving the objective of a good implementation of the exemption.

Additionally, we want to emphasize that VISA and Mastercard schemas set clear rules for acquiring PSPs for the information accompanying Card Payments, and the scheme determines the necessary Merchant Category Codes to be used. For the card issuer it is impossible to determine if the said MCC is correct or not. Due to this, the requirement for assessing MCC codes should be addressed to acquiring PSPs.

Currently only person-to-person card payments are in scope of the Transfer of Funds Regulation The proposed changes (looking into the Customers trends and behaviours, past payment histories etc. to determine whether the Card Payment is used for Payment of goods or services) would require card payment PSPs to monitor card payments in real time for determining if payment is deemed as the purchase of goods or services. This will affect the Card Payment-flows greatly. This will require major technical development for all PSPs and will incur a great financial cost.

Thus, we believe that the cost of implementing these changes may be disproportionate to the usefulness of these demands.

2.2. Linked transfers in relation to the 1000 EUR threshold (Article 2(5)(c), Article 5(2), Article 6(2) and Article 7(3) of Regulation (EU) 2023/1113)

Paragraph 8. c.

We are concerned that incorporating "smurfing techniques" may result in confusion with connected transactions that are not separated to circumvent the 1 000 EUR threshold. This amendment introduces a unclarity in the interpretation of the "links" to be considered for the application of the Regulation. We think that it would be preferable to remove the phrase "including the possible use of smurfing techniques" or to clarify that this rule should be applied in accordance with the associated risks.

3. Transmitting information with the transfer (Article 4, Article 5, Article 6 and Article 14 of Regulation (EU) 2023/1113)

3.2. Multi-intermediation and cross-border transfers

Paragraph 18.

We seek additional guidance on paragraph 18, as we find the obligations imposed on PSPs and IPSPs to be unclear in this paragraph.

3.3. Batch transfers (Article 6(1), Article 7(2) (c), Article 15, Article 16(1), Article 20 of Regulation (EU) 2023/1113)

Paragraph 19.

The paragraph introduces an "alternative channel mechanism," which is a new requirement for PSPs. Developing new technical mechanisms is expected to be costly and time-intensive, especially when there is no specification for the PSPs regarding the required technical standards. This lack of specificity may result in varied solutions across the EU, potentially impeding payment flows, particularly in relation with the SEPA Instant Payments Regulation.

Additionally, we think that the draft guideline misses the view of the Card Business. Visa and Mastercard do not support such alternative mechanisms, thus making such requirement for card issuing PSP's impossible to comply with.

PSPs commonly rely on SWIFT messages to seek additional information about payments. This method is widely used, is considered safe and secure, and aligns with General Data Protection Regulation (GDPR) requirements. It is recommended that this method be the exclusive method allowed in the future.

Certain payment institutions' business logic is based to collect and forward payments to banks in batches. The guideline provides too much room for interpretation regarding how the requirement for information sharing with banks should be met in the context of batch payments.

4. Information to be transmitted with the transfer (Article 4 and Article 14 of Regulation (EU) 2023/1113)

Paragraph 20.

Generally concerning paragraph 20, we believe that the notion of "error" could be specified because it seems too broad and could include situations that are not relevant to systematically report the errors. This amendment could lead to an excessive burden on PSPs and could hamper the straight-through processing of transfers of funds, as required under recommendation 16. We think it could also be applied on a risk-based approach and allow the institutions to define their own criteria, including the typologies of errors that are relevant to report.

Such manual work or resubmission is not possible in Visa and Mastercard card payments as all decisions need to be made online. We fear that extra validations during card payment process will make unnecessary and serious harm to acceptance and affect people's everyday lives at POIs.

Additionally, we wonder how a PSP could inform others in the payment chain if the SWIFT message does not reach all the participants of this payment chain. We kindly request clarification on the necessary tasks to detect the missing or incomplete information when an error is detected after the payment has already been processed. We would like to understand what PSPs actions could be considered sufficient.

Typically, the validation of the payment, and the controls to detect the meaningless, missing or incomplete information is performed technically as part of the payment process. Therefore, there is currently no easy way to make the detection (these tasks) separate of the overall technical payment flow.

In practice, the only way to make the required detection after the payment was processed is to resubmit the payment through the end-to-end payment process within the bank. This implies resending the payment, including repeating the settlement, which causes difficulties for all participants of the payment flow (as the payer's PSP needs to then send a recall etc.).

Another practical solution to fulfilling this requirement could involve implementing extra manual checks for these payment errors, which will impact the manual labor costs and hinder the detection tasks to be made (potentially extending the timeframe to days or even weeks, depending on the volume of errors).

4.1. Providing the payment account number of the payer (Article 4(1) point (b) of Regulation (EU) 2023/1113), and of the payee (Article 4(2) point (b) of Regulation (EU) 2023/1113)

Paragraph 21.

We do not consider it legally or technically possible to mix Card Payment processes to wire transfers processes (SEPA- and SEPA Instant payments).

If a payment is made using a card, the payment is only processed through Card payment schemas (i.e. VISA or Mastercard etc.) within the Card Payment Processes.

The PCI DSS standard is an obligatory requirement to secure card credentials and minimize risk of fraud. The full card number shall not be used in such scenarios as suggested in paragraph 21.

When a wire transfer is used (SEPA or SEPA Instant Payment), there are no card payments within the end-to-end process.

There is no current technical way to include card numbers in SEPA- or SEPA Instant payments. Taking into consideration the obligatory PCI DSS-standard, there is no possibility for the bank to use full payment card numbers (PAN) outside the card payment processes. There also should be no need to do so.
This question should be discussed with the international Card Schemas (Visa, Mastercard etc).

4.2. Providing the name of the payer (Article 4(1) point (a) of Regulation (EU) 2023/1113), of the payee (Article 4(2) point (a) of Regulation (EU) 2023/1113), of the originator (Article 14(1) point (a) of Regulation (EU) 2023/1113), and of the beneficiary (Article 14(2) point (a) of Regulation (EU) 2023/1113)

Paragraph 22. c.

The addition of the "the names of all holders of the account, address or wallet" introduces a major technical change for the payment processes, which is expected to be costly and time-intensive.

For example, in one Member State, there are accounts of estates that may involve several joint parties. If an account has multiple separate owners, this information may not be technically possible to add to the payment, as the utilized fields may not support such extensive data. We wonder if it is necessary to include all the joint parties' names in all the payments.

4.3. Providing the address, including the name of the country, official personal document number, and the customer identification number or, alternatively, date and place of birth of the payer (Article 4(1) point (c) of Regulation (EU) 2023/1113) and of the originator (Article 14(1) point (d) of Regulation (EU) 2023/1113)

Paragraph 23 and Paragraph 25: The address of the natural person

Aside from the individuals identified as vulnerable in Paragraph 23, there are also those whose address is designated as a P.O. box or "poste restante" for safety reasons, as stipulated in the national law of certain Member States. This category notably includes individuals at risk due to their professions (judges, police officers, bailiffs, reporters etc.) who have received personal threats or threats against their families. Additionally, individuals facing domestic dispute situations may require special protection due to the threat of violence. In such cases, the bank may be aware of the actual residence of these individuals, but in accordance with national law, it is obliged to keep this information confidential.

In these cases where the customer needs extra protection, the bank must use only the P.O. box or the poste restante-information in the payments.

We would like for these specific situations to be reflected in paragraph 23.

GDPR requirements should also be considered in relation to the new demands on Paragraphs 23 and 25-26.

Paragraph 27.

Paragraph 27 states that all the addresses of joint account holders should be included in the payment message. In line with the observation made in the comment on paragraph 22.c, we find that the payment message may lack sufficient space to accommodate several joint account owners.

5.3. Monitoring of transfers (Articles 7(2), Article 11(2), Article 16(1) and Article 20 of Regulation (EU) 2023/1113)

Paragraph 34. d.

EBA added some risk factors in these guidelines, notably on the implementation of FATF recommendation.

Although we acknowledge the risks associated with PSPs or VASPs in countries not adhering to FATF recommendations, we are concerned that this criterion might result in a situation of de-risking. This concern is particularly relevant if applied to PSPs, as it may be interpreted as a prohibition to systematically refuse transfers from countries that are implementing or have not implemented Recital 16.

The information published by FATF are crucial in the implementation of the risk-based approach. However, it is not the role of financial institutions to regularly assess the implementation of FATF country recommendations. Additionally, assessing the technical compliance of local regulations with FATF recommendations can pose challenges in low-capacity countries due to limited access to regulations.

However, it is relevant for VA related activities to take into account in the risk assessment of VASP the quality of the regulation and their supervision. The drafting could rather focus on the existence of a regulation or supervision rather than referring to the implementation of FATF recommendation.