European Payment Institutions Federation aisbl

European Payment Institutions Federation

July 2020

EPIF's response to EBA Revised Guidelines on ML/TF risk factors

Instructions

The EBA invite comments **only on the amendments and additions** to the original risk factors Guidelines, which will be repealed and replaced with the revised Guidelines.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- are supported by a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- provide alternative regulatory options for consideration by the EBA.

General Guidelines

General Comments on Title I on generic Guidelines :

EPIF is pleased to have the opportunity to provide comments for the EBA Revised Guidelines on ML/TF risk factors.

Although the EBA revised Guidelines will significantly improve and help all the obliged entities to take the necessary steps to identify and assess the ML/FT risk, we ask the EBA to take into consideration our recommendations to ensure their ongoing accuracy and relevance, moreover because the risk can vary in each EU member state and according to the different sectorial or business model they represent.

As a general comment, we agree with the generic Guidelines in Title I, but we would like to include some specific comments about cash withdrawals/ATMs, transaction monitoring, record keeping and independent audit that firms should take into consideration to tackle potential emerging risks.

We welcome, among other recommendations mentioned in this document, the addition of sector-specific Guidelines to the Risk Factor Guidelines (Title II) but would like to ask to include certain additional sectors (credit or charge card companies), not specifically considered in the revised Guidelines.

Finally, as stated in the revised Guidelines, together Title I and Title II promote the development of a common understanding, by firms and competent authorities across the EU, of what the assessment of ML/TF risk entails and how it should be conducted. Nevertheless, we would consider it generally helpful if the EBA were to also consider issuing guidelines for other business models and, in addition, to review areas of EU law that are not fully harmonized or are not yet addressed by EU law.

General Comments on Title II on sector specific Guidelines :

We welcome the addition of sector-specific Guidelines to the Risk Factor Guidelines. In this regard, we suggest that the EBA considers including guidance for additional business models, namely credit and charge card issuers. This would promote effective risk management and support firms' AML/CTF

compliance efforts, enhancing the ability of the EU´s credit and charge card sector effectively to deter and detect ML/TF by means of guidance on:

- business-wide and individual ML/TF risk assessments;
- customer due diligence measures including on the beneficial owner;
- terrorist financing risk factors; and
- emerging risks, such as the use of innovative solutions for CDD purposes

In that regards, FATF and Wolfsberg issued similar documents:

1. Prepaid cards, mobile payments and internet-based payment services (June 2013)
2. Wolfsberg AML Guidance on Credit/Charge Card Issuing and Merchant Acquiring Activities (2009)

Additionally, this new guidance for credit and charge card companies would help reduce competitive disadvantage versus other financial companies under similar AML regulations in EU, especially if EU competent authorities were to set supervisory expectations of firms by reference to the guidance, rather than for example requiring compliance with the same standards applicable to generally much higher risk entities such as banks who might also happen to issue credit or charge cards. This type of guidance would help supervisors to communicate and set clear expectations of the factors firms should consider when identifying and assessing ML/TF risk and deciding on the appropriate level of CDD.

1. **Do you have any comments with the proposed changes to the Definitions section of the Guidelines?**

2. **Do you have any comments on the proposed amendments to Guideline 1 on risk assessment?**

3. **Do you have any comments on the proposed amendments to Guideline 2 on identifying ML/TF risk factors?**

   According to FATF (http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf) access to cash through the international ATMs (some of them based in high risk countries) or national ATM network increases the level of ML/TF risk. In our view, the revised Guidelines focus on cash withdrawal only in two sectors (Sectoral guideline for electronic money issuers and crowdfunding) and don´t consider other industries/firms where this factor may contribute to elevated customer risk. For example, the use of ATMs by retail bank or wealth management firm customers, which gives them access to a global ATM network that allows high-value cash withdrawals or multiple withdrawals in a short period of time and without an economic rationale. In our view the ability to use ATMs in relation to a product should be included as a risk factor when identifying the risk associated with it, and the involvement of an ATM is also relevant to the assessment of an individual transaction as suspicious or not.

   In addition, the guideline proposes to consider a lack of face-to-face interaction (or avoidance thereof) as a risk factor. For online businesses where by definition there is no face-to-face due diligence, we would suggest that this wording is expanded to include a customer attempting to avoid due diligence altogether or, where various non face-to-face CDD options are available, refusing to comply with the more direct and personal options such as face matching or live selfies.

4. Do you have any comments on the proposed amendments and additions in Guideline 4 on CCD measures to be applied by all firms?

One of the main requirements of any transaction monitoring program is that its efficacy should be kept under regular review (Guideline #7 and chapter 4.72: Firms should ensure that their approach to transaction monitoring is effective and appropriate). In addition to the different proposals included in Guideline 4 (Transaction monitoring, chapters 4.72 to 4.74), our suggestion would be to explore the possibility of allowing disclosure of information between two or more entities about a shared customer or transaction (regardless of the professional category/sector) as long as those entities are under the same AML regime and subject to equivalent obligations as regards professional secrecy and personal data protection. The information exchanged would be used exclusively for the purposes of the prevention of money laundering and terrorist financing and would be disclosed by the AML Compliance Department. Ideally, this type of disclosure would also be permitted between firms domiciled in the European Union or in equivalent third countries (in terms of their AML, professional secrecy and data protection standards). Naturally, it would not extend to disclosure to entities domiciled in third countries not classified as equivalent.

We welcome the EBA's recognition, at Guideline 4.32, that Directive (EU) 2015/849 is technology neutral with respect to customer verification.

As firms are best placed to assess the risks they are exposed to, they are best placed to identify the solutions to those risks. We therefore welcome the obligation for Firms to assess the efficacy of technology solutions utilized by them (Guideline 4.33).

New technologies, when applied appropriately, represent an opportunity to address and reduce ML/TF risks as they enable firms to take account of additional data points and to robustly scrutinize information provided by financial services users. As the financial services industry continues to develop, the need for non-face to face verification continues to rise. Non-face to face verification is essential to facilitate financial inclusion and competition among firms (by way of reducing barriers to market entry).

While we accept firms must be in a position to demonstrate the appropriateness of technological solutions adopted by them (as set out in Guideline 4.36), we ask that confirmation is provided with regard to when firms will be required to do so. We are of the view that firms should not be required to obtain prior approval from Competent Authorities regarding the use of a particular technology solution but rather be required to demonstrate the appropriateness of the solution after implementation. This will enable ML/TF mitigation measures to keep pace with risks that continually develop. However, we recognize that firms will need to have robust governance and testing in place to facilitate this approach.

We would further strongly encourage CAs to develop a forum where they can inform each other and exchange know-how of such best practices employed by firms in their respective jurisdictions

With regards to **beneficial ownership and control** – frequently when onboarding or reviewing a multinational customer organization, where complex ownership structures are the norm rather than the exception, challenges arise around the legal declaration that there is no beneficial owner or individual who exercises control over the customer. We suggest adding a reference to large corporates with complex structures where it is reasonable to conclude that there is no beneficial owner, rather than expending excessive effort on a fruitless search.

On **SDD**, the possible threshold utilized before enforcing full due diligence must be directly tied and proportionate to the firm's assessment of the customer risk profile. There is no "one size fits all" approach to SDD thresholds. SDD must also be supported by other elements of a holistic controls framework, such as transaction monitoring.

It would be useful if the due diligence guidelines can clarify the amount of "informal reliance" firms can place on the fact that a customer holds a verified account with another financial institution subject to the same regulatory framework. This should not and cannot be the only factor considered, but rather a form of additional confirmation and assurance that the customer has gone through the due diligence process at another financial institution.

5. Do you have any comments on the amendments to Guideline 5 on record keeping?

The European Banking Authority (EBA) published last October a report identifying potential impediments to the cross-border provision of banking and payment services in the EU. Developed under the EBA's FinTech Roadmap, this Report calls on the European Commission to facilitate cross-border access, including the update of interpretative communications on the cross-border provision of services and further harmonisation of consumer protection, conduct of business and AML/CFT requirements, in order to facilitate the scaling up of activity cross-border.

In order to allow passporting firms to comply with record keeping obligations and demonstrate to their competent authority that the measures taken are adequate, areas of EU AML law should be harmonized to the maximum extent possible. As an example, some EU countries require firms to keep documents for 10 years (Spain or Italy) and other EU countries only 5 years (France) after the relationship or professional service has ended, or the carrying out of the transaction. We would suggest that the EBA considers advising EU policy makers on a harmonized approach, in order to remove obstacles that impede the operation of the Single Market in payment services. Therefore, harmonization about the record keeping requirements should be consistent across EU, moreover whenever there are firms passporting their services in different EU markets.

6. Do you have any comments on Guideline 6 on training?

7. Do you have any comments on the amendments to Guideline 7 on reviewing effectiveness?

Unless required by the local AML/TF regulation (for example, in Spain since 2005), we submit that an independent review should only be required whenever the second or third line of defense detect potential high-risk issues that directly impact the firm´s risk profile. This independent review should focus only on specific AML controls (for example, EDD process or Transaction Monitoring), rather than the complete AML program. As well as being a more proportionate approach, this would also reduce the cost of implementation of this recommendation for firms.

Sector specific guidelines

8. **Do you have any comments on the proposed amendments to Guideline 10 for electronic money issuers?** –

Some electronic money products are created to support sections of the population which are unbanked or who have less access to traditional banking products. Due diligence and monitoring for such customers needs to take into account financial inclusion and a risk-based approach for EMI firms.

For factors that may reduce risk: products that represent a "closed loop" where funds can only be used for a specific purpose or with a limited number of approved merchants (building on the existing bullet 10.5 c) iii.)

In the section around factors that may contribute to increasing risk: multiple different customers who present similarities in their data which may indicate that those accounts are being controlled by one person (e.g. IP or device data).

The threshold mentioned in 10.18 a) of 150 EUR for SDD low risk scenarios goes beyond the threshold in Article 12 of Directive (EU) 2015/849 which was 250 EUR. We find this excessively restrictive and in contradiction with the drive for a risk-based approach where we believe a holistic and strict controls framework can enable higher thresholds for Simplified Due Diligence.

9. **Do you have any comments on the proposed amendments to Guideline 11 for money remitters?**

10. **Do you have any comments on the additional sector-specific Guideline 18 on account information and payment initiation service providers?**

EPIF welcomes the addition of sector-specific Guidelines to the Risk Factor Guidelines, but would like to ask that the guidelines remain risk and principle based and do not exclude certain business models by making statements that rule out any other market practice.

The market for AIS and PIS services in particular is still in an early stage of development and many business models may yet arise which address a particular market need. PIS services specifically can be applied in a variety of market environments: a PISP may offer its services to account holders, consumers to enable them to pay another consumer for the purchase of a good on a marketplace, but may also offer the same services to an online merchant to enable it to accept payments via payment initiation / credit transfer. In the latter model, the Payer will not be a customer of the PISP as its relationship is with the online merchant only to enable payment acceptance in the same way as e.g. card acquirers do.

The Guidelines should not state as strongly that 'For PISPs: the customer is the natural or legal person who holds the payment account and request the initiation of a payment order from that account the (Payment service user)' but rather state that 'For PISPs: multiple business models can exist where the customer can either be the natural or legal person who holds the payment account and request the initiation of a payment order from that account the (Payment service user) in case of a stand alone PIS, but where the PIS is provided to a merchant, the customer can be that merchant with the Payment service user not always being a customer as well.

With regard to the sector specific Guidelines for TPPs, it is important to recognise that there are various PIS models in the market, and it will not be appropriate for all PIS models to need to conduct due diligence on the payer.

To give more colour, in a pure PIS journey, the PISP does not hold any funds to execute the payment themselves, rather they simply provide the technology to connect a payer to their ASPSP and provide the recipient's bank details to the payer's ASPSP, which single-handedly executes the payment and itself is subject to AML obligations.

In some PIS models, the PISP contracts with Merchants to facilitate ecommerce transactions. All due diligence and KYC is done on the merchant, as there is an ongoing relationship.

The PISP only facilitates the transaction for the merchant on behalf of the payer via the bank, there is no ongoing relationship with the payer and therefore no ability or need to conduct due diligence.

Based on the OBIE's technical specifications, a pure PISP will receive data on currency, amount of the transaction, classification of transaction and in certain instances the shipping address from the merchant.

There is insufficient information for a PISP to do any KYC, have an ongoing relationship with the payer, or connect future transactions by the same payer to identify linked transactions.

The ASPSP would have already conducted KYC checks on the payer prior to setting up the payers current account. They are best positioned to identify unauthorized access and transaction monitoring on the payers account. SCA and existing fraud alerts already exist and are leveraged by the ASPSP.

In the instance of a pure PIS, the merchant is the customer of the PISP, whom they have an established relationship and whose name they obviously know.

We believe that the PIS Guidelines must include reference to different models such as where a PISP contracts with the Merchant and does not execute due diligence on the payer. The guidelines should not contain an expectation for the PISP in such a flow to complete due diligence on the payer.

This should also include reference to return flows from the merchant back to the payer in case of refunds or payouts – as above, the PISP does not hold the funds or the relationship with the payer but only triggers the transaction between the two accounts.

Risk factors such as payments triggered from different accounts are difficult (or impossible) to apply where the PISP does not have a customer account or perform due diligence on the payer.

All guidelines for due diligence in this form of Payment Initiation Service should focus on the due diligence applied to the merchant (generally the recipient) by the PISP.

Generally, the risk associated with the transaction flow should be considered as low (especially within the EEA) due to the fact that payments are initiated from a valid payment account held at a regulated financial institution.

As the EBA acknowledged in its consultation, AISPs do not provide payments and are not involved in the payment chain; they are simply information service providers. AISPs have read-only access to customer bank account information and neither the AISP nor the AISP's customer can conduct financial transactions on a bank account from within the pure AISP environment. Application of AML requirements to AISPs would not have the effect of restricting the flow of illicit finance as there is no chance for money laundering or terrorist financing to occur via an AISP platform. AML obligations

properly sit with the financial institution (i.e. the bank/ASPSP) which provides the accounts in relation to which an AISP provides information services; this is where the transactions take place and where the relevant business relationship with the customer exists.

Ultimately, the AML framework covers the provision of PIS and AIS only in cases, when these services are provided by AISP or PISP as a part of another service eventually consisting in a transaction. However, in the scenarios where AIS or PIS is provided independently, the provision of these services should not lead to imposing AML obligations on AISP or PISP as it neither constitutes execution of a transaction nor creation of conditions for transaction execution. The exclusion of the AML regime in relation to AIS and PIS provided without any connection to the activity constituting the transaction of the service provider for the account holder is consistent with the AML framework and the current understanding of payment services as provided for by PSD2. The approach excluding the application of the AML regime to specific services based on their nature and economic purpose does not constitute an attempt to circumvent the AML requirements. That is so because activities that do not consist in carrying out a transaction or are not related thereto are increasingly being introduced to payment and banking services. For this reason, given the objectives of the AML system and a variety of potential business models, it is necessary to make a case-by-case assessment of whether a particular service or part of it is subject to AML regulations or not.