08/07/2020

Consultation Input on EBA Draft Guidelines:

Revised money laundering and terrorist financing (ML/TF) risk factors

Introduction

The EBA issued a public consultation on revised money laundering and terrorist financing (ML/TF) risk factors Guidelines as part of a broader communication on AML/CFT issues. This update takes into account changes to the EU Anti Money Laundering and Counter Terrorism Financing (AML/CFT) legal framework and new ML/TF risks, including those identified by the EBA's implementation reviews. These Guidelines are central to the EBA's work to lead, coordinate and monitor the fight against money laundering and terrorist financing, explained in the accompanying factsheet. The according market consultation ended on 06 July 2020, when the European FinTech Association provided the following input to the EBA.

The according market consultation ended on 06 July 2020, when the European FinTech Association provided the following input to the EBA.

Response Details

Question 1: Do you have any comments with the proposed changes to the definitions section of the guidelines?

The European FinTech Association (in the following also referred to as EFA) has no comments on the proposed changes to the definitions section of the Guidelines.

Question 2: Do you have any comments on the proposed amendments to guideline 1 on risk assessment?

The EFA has no comments on the proposed amendments to Guideline 1.

Question 3: Do you have any comments on the proposed amendments to guideline 2 on identifying ML/TF risk factors?

We think that there should be further explanation in terms of the impact of tech/data has on the identification of ML/TF risk. A key factor in the identification of ML/TF has become the effective utilization of tech advancements, this needs to be considered and become a core tenet of an effective structure against ML/TF.

EFA | European FinTech Association a.s.b.l
Rue Washington 40
1050 Brussels, Belgium

Commercial/Association register number: 0741.453.152
EU Transparency Register: 514240237898-38

www.eufintechs.com
admin@eufintechs.com

In addition there is a lack of focus on actually review and practical application of patterns/typologies and investigative methods. The guideline may be too basic to actually identify sophisticated financial crime.

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

Our recommendation is to also add further granularity and explanation on the extended data points that exist such as IP-Address, Geolocation and Device ID. In addition, there should be further clarification of what constitutes high risk activity and high risk industries in context of CDD/EDD. The focus is still too large on country-based risk, which has been not the most prevalent indicator of potential financial crime activity. www.eufintechs.com European FinTech Association 3 It should be clarified in the No. 4.29 et seq. that digital identifications should not per se be seen as less safe or trigger enhanced measures of due diligence. In our experience it is not correct to generally establish a preference for face-to-face identification - as is implied in No. 4.29 et seq. Giving preference to face-to-face identification leads to a discrimination of digital service providers as they do not offer face-to-face identification, i.e. they do not provide a level-playing-field. National regulators use this provision to establish stricter measures of customer due diligence for digital business models than for established service providers. We believe that there are benefits in providing services digitally - it gives people access to services remotely that they would otherwise not have had, can be easily supervised as the flow is fully transparent and online and advances cross-border services within the EU - which is in line with the priorities of the European integration. The EBA should consider at least allowing certain highly safeguarded and at the same time digitally workable identification methods such as the identification via reference transaction as not triggering enhanced measures of due diligence.

Question 5: Do you have any comments on the amendments to guideline 5 on record keeping?

The EFA has no comments on the proposed amendments to Guideline 5.

Question 6: Do you have any comments on guideline 6 on training?

The EFA's recommendation is also to add unusual/suspicious behavior as this also covers internal fraud as well as all possible activity in affected firms.

Question 7: Do you have any comments on the amendments to guideline 7 on reviewing effectiveness?

Regarding the Guideline 7 EFA recommends that any effectiveness review should at best be part of the risk assessment of a firm. Independent risk assessments and effectiveness reviews do not foster a coherent and sustainable risk-based approach.

Moreover, an independent review of the effectiveness of a risk assessment approach should lie with the statutory auditor. If there is tangible evidence for a lack of effectiveness, a statutory auditor MUST identify it. The EBA should refrain from recommending independent reviews by third parties which are not statutory auditors thus weakening responsibilities of the latter.

Based on the recent Wolfsberg Paper and the overall importance of this subject this guideline should be expanded to better highlight for affected parties how effectiveness is measured. All the guidelines prior should be brought together in this one. Being effective as a firm means in our opinion to deploy the right technical foundation with the required expertise in the trained staff acting in a regulatory environment that is focusing on effective measures to prevent financial crime, which can include measures such as concrete suspicious activity reporting guidelines.

The relation of effectiveness versus regulatory obligations in these guidelines do not reflect the actual challenges of firms.

Question 8: Do you have any comments on the proposed amendments to guideline 8 for correspondent banks?

The EFA has no specific comments on the proposed amendments to Guideline 8.

Question 9: Do you have any comments on the proposed amendments to guideline 9 for retail banks?

Apart from the other points mentioned above, our proposed amendments here are focused on the increased risk of non-face-to-face relationships. Due to the utilization of technology in verification the ability to detect fraudulent behaviour is much higher than with traditional face-to-face identification. The key in our opinion is to highlight the necessary steps to ensure high quality non-face-to-face identification, which has to include the utilization of the digital ID and compilation of internal as well as external data points. The proposed provisions discriminate digital business models and give preference to incumbents with large networks of local branches. They are neither modern nor based on a thorough analysis of facts. Digital identifications have many benefits for the consumer, the service provider, but also for the regulator. They are fully auditable and objective, whereas a face-to-face identification is always only as safe as the person performing the identification.

In addition the biggest area of concern for financial institutions are the rise of money mules created from social engineered, stolen, faked identities. This concern is not reflected in the guideline and should be considered to be added in detail to the guideline, as this is an industry-wide effort to solve.

Further, we do not see that reliance on a third party as indicated in No. 9.1 should contribute to risk. To the contrary third party reliance is actually a measure to double the efforts in fighting money laundering. The exchange of information should be encouraged, not discouraged. At the same time third party reliance is an important measure in case of B2B cooperations between Fintechs, but also between Fintechs and banks. In particular in cross-border situations reliance plays an important role to enable business relationship as e.g. a Portuguese bank may rely on a Dutch bank for the identification of a customer. Applying local AML identification rules in these cases oftentimes does not work as people are used to their local types of identification methods.

No. 9.6 lit. a) vi) should be amended to exclude EU citizens. This provisions discriminates against the crossborder provision of services, i.e. offering of a simple bank account from a bank in one EU state to a customer in another EU state. It hinders the cross-border provision of services and therefore truly European

business models. It is also not appropriate. Why should the opening of a bank account with a digital service provider in another EU member state should be considered a risk factor in a digital single market?

Question 10: Do you have any comments on the proposed amendments to guideline 10 for electronic money issuers?

The EFA has no specific comments on the proposed amendments to Guideline 10.

Question 11: Do you have any comments on the proposed amendments to guideline 11 for money remitters?

The EFA has no specific comments on the proposed amendments to Guideline 11.

Question 12: Do you have any comments on the proposed amendments to guideline 12 for wealth management?

The EFA has no specific comments on the proposed amendments to Guideline 12.

Question 13: Do you have any comments on the proposed amendments to guideline 13 for trade finance providers?

The EFA has no specific comments on the proposed amendments to Guideline 13.

Question 14: Do you have any comments on the proposed amendments to guideline 14 for life insurance undertakings?

The EFA has no specific comments on the proposed amendments to Guideline 14.

Question 15: Do you have any comments on the proposed amendments to guideline 15 for investment firms?

The EFA has no specific comments on the proposed amendments to Guideline 15.

Question 16: Do you have any comments on the proposed amendments to guideline 16 for providers of investment funds and the definition of customer in this Guideline?

The EFA has no specific comments on the proposed amendments to Guideline 16.

Question 17: Do you have any comments on the additional sector-specific Guideline 17 on crowdfunding platforms?

The EFA has no specific comments on the proposed amendments to Guideline 17.

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

A. Summary

Legal and regulatory provisions for TPPs that are far beyond risk-based and proportionality principles can endanger a successful open banking market in Europe. A current example is AML regulation for TPPs. AML rules should apply to cases where business models have a clear connection with money laundering risks. For example, where businesses are responsible for executing transactions and come into possession of customer funds.

When the new Payment Services of Account Information Service (AIS) and Payment Initiation Service (PIS) were introduced by PSD2, providers of both services were automatically classed as obliged entities under AMLD, despite the fact that neither type of provider executes transactions or comes into possession of funds.

As the EBA itself acknowledges in its Draft Guidelines "the inherent ML/TF risk associated with [these services] is limited" for these very reasons. The inclusion of these services needs to be re-examined as part of the Commission's AML action plan, to remove duplication and friction which will ultimately prevent consumer take-up of these innovative new services and hamper innovation and competition.

We ask that the EBA's Risk Sector AML Guidelines are not finalised until the conclusion of the Commission's consultation - particularly given the contention around whether AIS and PIS were intended to be included as obliged entities, or whether this was the unintentional result of cross referencing between PSD2, CRD and AMLD.

If, despite their low risk, PISPs were to remain in scope of AMLD, a number of changes need to be made to ensure PIS business models remain viable:

- Since PISPs' primary relationship is with the online merchant (with whom they contract to provide the regulated service) it should be clarified that AML due diligence is required to be carried out on the PISPs merchant client, and not on every PSU who makes purchases from the merchant via PIS. To do otherwise will hugely and unnecessarily disadvantage PISPs compared to other payment methods, who are not under this obligation.
- If PISPs are to be required to undertake transaction monitoring, banks should be required to return certain information about the PSU to the PISP including via PSD2 interface/API (BIC, IBAN, and name of the account holder). This is necessary to allow PISPs to uniquely identify transactions, without adding extra dissuasive steps into the PSU's payment experience.

B. General comments

All 'Financial Institutions' are subject to the anti-money laundering requirements. 'Financial Institutions' are defined as those carrying out one or more of the listed activities set out in points 2 to 12, 14 and 15 of Annex 1 to the Capital Requirements Directive (CRD, Directive EU 2013/36 EU). Point 4 of the Annex to CRD previously included payment services as defined under PSD1 (Directive 2007/64 EC). PSD2 (Article 113, Directive 2015/2366 EU) updated Point 4 of CRD to include the new list of payment services in PSD2, which includes AIS

and PIS and brought these services into the scope of AML, possibly without intent or at least without a thorough investigation of its unintended consequences. The EFA requests that before any specific AML guidelines for AIS and PIS providers are finalised, there should be a more fundamental discussion, as to whether there is a need to include these services in the scope of the AML requirements.

Nevertheless, we provide some general comments drawing out the negative impacts of the EBA Guideline 18 in the following.

The EBA consultation acknowledges that they and other ESAs 'consider that the ML/TF risk associated with their activities is limited'. However, it then proposes some actions for AISPs and PISPs which do not meet this fact. In contradiction, those actions would prove extremely burdensome, and go beyond what these businesses would usually do to provide open banking services:

- As part of their CDD processes, PISPs and AISPs should ensure that their AML/CFT systems are set up in a way that alerts them to unusual or suspicious transactions. Even without holding significant information on the customer, PISPs and AISPs should use their own, or third party typologies, to detect unusual transactional activity.
- PISPs and AISPs should apply CDD measures to their customers (which are clarified as the payment service user).
- Each time an account is added, the AISP should ask the customer whether the account is his own account, a shared account, or a legal entity's account to which the customer has a mandate to access (e.g.: an association, a corporate account).

The EFA has concerns that these requirements are:

- Disproportionate and not compatible with existing law (PSD2).
- A risk to the take-up of open banking services and the competition objectives of PSD2.

i. Disproportionate and not compatible with existing law (PSD2)

The European Commission noted in its press release in January 2018, that PSD2 was intended to 'help stimulate competition....[that] would then allow consumers to benefit from more and better choices between different types of payment services and service providers'.

However, asking new providers of AIS and PIS to serve a separate purpose - to be watchdogs for illegal money flows through the ASPSs - is disproportionate, and was never initially outlined as an objective of PSD2.

Third party providers under PSD2 are specifically required by law to apply strong data minimization principles using data for account information services. As Article 67(f) makes clear, AISPs must 'not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules. These TPP-specific data minimization principles would be counteracted by the new guideline 18.

ii. Risk to the take-up of Open Banking

Requirements on AISPs and PISPs to conduct due diligence (CDD) and verification (e.g. proof of identity and address checks) would dissuade many PSUs from using the services in the first place. PSUs will wonder why

they have to repeat the KYC process to allow an AISP to access their payment account transaction data, having already done this to open their payment account in the first place. Requirements to notify authorities of suspicious transactions would require each AISP and PISP to build costly systems, and, even if feasible, would lead to double counting of reports already received from ASPSPs. The cumulative impact of these requirements could lead businesses to exit the emerging open banking market before it has taken off.

Additionally, authorities have supported PISPs to encourage competition with card schemes and reduce merchant fees alongside the Interchange Fee Regulations. If PISPs have to stop customers mid-checkout to ask for proof of identity and address documents (which incidentally is not a requirement for card acceptance), opportunities for competition and innovation in payments will be snubbed out.

C. Specific Comments regarding Measures According to the proposed Guideline 18.8 the customer is:

a) 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).

b) For AISPs: the customer is the natural or legal person who has the contract with the AISP. This can be the natural or legal person who holds the payment account(s).

i. Concerning: 18.8(a)

Clarifying that the customer of the PISP is the PSU sets an expectation that PISPs will need to conduct CDD on the PSU. This will be damaging to PISPs who contract only with merchants. The PSU would have to be stopped at the online check-out to perform CDD with the PISP. This would dissuade any PSU from using PIS to make payments, because they would be able to make payments using card (and they would not have to undergo CDD at the checkout using this method). This creates an unlevel playing field and defeats one of the objectives of PSD2 - to support payment methods to compete with cards.

Under PSD2, PISPs do not have a contract with the PSU (framework contracts govern the execution of transactions, not the initiation of transactions - as per PSD2 Article 4(21)). Instead, the customer of the PISP will usually be the merchant - as discussed in recital 21 of PSD2:

"In particular, payment initiation services in the field of e-commerce have evolved. Those payment services play a part in e-commerce payments by establishing a software bridge between the website of the merchant and the online banking platform of the payer's account servicing payment service provider in order to initiate internet payments on the basis of a credit transfer."

Accordingly, the account owner (PSU) is not the "customer" of the PISP in the sense of AML. The PISP does not establish a "business relationship" with the account owner in the sense of Art. 11 (a) AMLDirective. CDD, therefore, cannot refer to the account owner.

This has been confirmed by the ESAs in charge of licensing PISPs: While PISPs need to provide documentation of their internal AML control mechanisms under Art. 5 (1) lit k PSD2, this has not referred to the identification of account-owners, but to the identification and CDD of online-merchants.

We suggest the EBA Guideline 18.8(a) should be read as follows:

For PISPs: The customer is the online-merchant (the payee) that is offering PIS as a payment alternative, e.g. on a website.

ii. Concerning: 18.8(b)

Clarifying that the customer of the AISP is the PSU sets an expectation that AISPs will need to conduct CDD on the PSU. Conducting due diligence and verification (e.g. proof of identity and address checks) would dissuade many customers from using AIS in the first place. Customers will wonder why they have to repeat the KYC process to allow an AISP to access their payment account transaction data, having already done this to open their payment account with their ASPSP. The cumulative impact of these requirements will lead businesses to exit the emerging open banking market before it has taken off.

Question 19: Do you have any comments on the additional sector-specific Guideline 19 on currency exchanges?

The EFA has no specific comments on the proposed amendments to Guideline 19.

Question 20: Do you have any comments on the additional sector-specific Guideline 20 on corporate finance?

The EFA has no specific comments on the proposed amendments to Guideline 20.