Electronic Money Association
Crescent House
5 The Crescent
Surbiton
Surrey
KT6 4BN
United Kingdom
Telephone: +44 (0) 20 8399 2066
Facsimile: +44 (0) 870 762 5063
www.e-ma.org

José Manuel Campa
Chairman
European Banking Authority
EUROPLAZA
20 Avenue André Prothin
92927 Paris La Défense
France

6 July, 2020

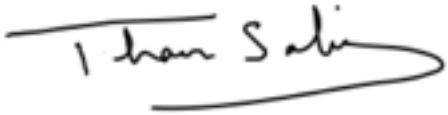
Dear José,

Re: EBA revised Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (''The Risk Factors Guidelines''), amending Guidelines JC/2017/37.

The Electronic Money Association is the trade body for electronic money issuers and innovative payment service providers. Our members include leading payments and e-commerce businesses worldwide, representing online payments, card-based products, vouchers, and those employing mobile channels of payment. We also represent a growing number of TPPs – both PISPs and AISPs. Please find full list of our members attached to this letter.

We welcome the opportunity to respond to the EBA's consultation on revised Draft Guidelines on CDD and AML-TF risk factors, amending Guidelines JC/2017/37. A number of proposed Guidelines will have a significant detrimental impact on our members, in particular the AIS and PIS providers, with little AML-TF benefit; we would be very grateful if you could take our concerns into account.

Kind regards



Thaer Sabri
Chief Executive Officer
Electronic Money Association

1. **Response in relation to sectoral guidance for electronic money issuers**

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

Comments on Guideline 10:

- **10.4(a)(ii)** Deletion of 'unlimited' number of payments is supported, and we suggest that the provision for 'high number of payments, loading or redemptions' be qualified with "where the aggregate amounts are also high". This is because payments for small value digital services such as in-game payments, music and similar services may be characterised by a high number of payments, but the total value transacted would be low, without giving rise to increased risk.
- **10.4(b)(ii)** Suggests that funding with payments from unidentified third parties is a factor increasing risk. For clarity, we would like to distinguish receipt of payments from third parties, as may be the case for a merchant receiving payments from customers, from the purchase of e-money for the purposes of funding the account.
- **10.5(b)** Provides that funding an e-money account using funds 'verifiably' drawn from an account held in the customer's sole or joint name is a factor reducing risk; this is a helpful addition, and would be further assisted if this can be broadened to include arrangements where control over the account by the customer is also established. This would have required the customer to have undergone the same level of CDD with the service provider and would provide a comparable level of risk mitigation. Addition of 'or is verifiably under the control of the customer' would assist.
- **10.5(c)** Proposes that domestic use of a product presents a lower risk than its use on a cross border basis. We believe e-commerce transactions have normalised cross border business, and this is the expectation for online services operated within single market. We suggest that this is expressed as 'the product cannot be used to make payments to high risk jurisdictions', rather than a general increase in risk as a result of cross border transactions.
- **10.6(a)** This a description of a typology with a number of component activities; it may be better addressed as a typology in a different setting rather than as a risk factor in the Guidelines. If it is retained, then the essence of there being no commercial or economic rationale to transactions may provide a suitably broad indication of the risk to be captured.
- **10.9 A** point of clarification, we assume that reference to a 'distribution agreement' is a reference to a merchant acquiring agreement for e-money services, rather than an agreement for the distribution of e-money. Confirmation would be helpful.

- **10.11(a)** The owner of the e-money has been identified as the focus of CDD measures. This is of course subject to there being a business relationship with the customer, or the customer undertaking qualifying occasional transaction(s). Reference to triggers for verification would be helpful.
- **10.15** High risk third countries (HRTC): this refers to Title 1 provisions set out at paragraphs 4.53 to 4.57. In turn, these clarify that relevant transactions that involve HRTC include funds that are generated in an HRTC, or funds that are received from an HRTC, or funds where the destination is an HRTC or the person with whom the firm is dealing is resident or established in an HRTC.
- Implementation of this obligation could be expressed in risk sensitive terms, where the value of the transaction would be taken into account, or the type of product is considered. An national of an HRTC country visiting the EU could purchase a prepaid card product for use as a tourist in the EU, and it is arguable that this should not give rise to EDD obligations set out at Article 18a of 4MLD as amended by 5MLD.
- Paragraph 10.15 could be elaborated to state that EDD is a risk-based requirement and that assessment must be subject to a full range of factors including the product proposition.
- **10.18(a)** This provides for examples of approaches to SDD, and addresses the postponement of verification. Identification would however have been undertaken at the outset.
- We are concerned that the provision introduces a monetary limit on aggregate transactions before verification needs to be undertaken. We find this provision problematic, it limits the opportunities for business to use postponement in a pragmatic manner that is risk based, that assists businesses, and it restricts the flexibility offered by level 1 text in 4MLD and 5MLD. Our objections are set out below:
    i. The aggregate limit adopted is identical to that provided under the exclusion provisions set out at Article 12 of 4MLD, where there is no requirement to identify the customer up to that limit or to undertake CDD, with the exception of monitoring. It is disproportionate therefore that where identification is undertaken, ongoing monitoring and other data is collected about the customer, that issuers should be restricted to the same aggregate spend as that provided for exclusion.
    ii. Given that this is a regime that is intended to be risk based, a fixed limit is by definition not risk based. It does not take mitigating measures into account, it does not allow for restrictions on product functionality, nor does it take consumer or business need into account, or those of financially excluded individuals.

iii. We note that the legislator chose to adopt a monetary limit for the application of exclusion from CDD under Article 12, but did not do so for Articles 15 on simplified due diligence, nor Article 18 for enhanced due diligence. The choice of the EUR 150 in the Article 12 exclusion was subject to considerable debate and consultation during the legislative adoption process and right up to the point of Parliamentary approval. Whilst the EBA is consulting on this provision, the decision is entirely that of the EBA and its supervisory board; neither industry, nor elected political representatives have any say in the decision making. This frustrates the efforts of all the parties that participated in the adoption of Level 1 text.

iv. We believe the application for such a restriction, by level 2 text, when the legislator chose not to do so, and specifically when the regime is intended to be risk based and proportionate to the risk posed is contrary to the objectives of the Directive, in that it restricts the ability to apply a risk based approach and to act in a proportionate manner. We request that this guideline is referred to the CJEU for an opinion. We request that the EBA does so on its own initiative.

v. We refer the EBA to Recital 7 of 4MLD where the legislator makes it clear that in the event of Article 12 not applying, electronic money issuers should be able to benefit from the provisions, of Article 15, subject to the risk being low. There would be little benefit in such a reference, if the aggregate limit for spending is identical.

   The text states: “Such an exemption should be without prejudice to the discretion given to Member States to allow obliged entities to apply simplified customer due diligence measures to other electronic money products posing lower risks, in accordance with Article 15.”

vi. We acknowledge that there are other limits set out at Article 12, such as excluding products that allow person to person transfers, or those funded with cash, whereas Article 15 does not require such restrictions. Had the legislator intended to address itself solely to products that did not meet these restrictions, then it would have been far simpler to draft a single Article removing all limits and simply providing that low risk must exist and an aggregate limit be imposed. This is clearly not the case, and the objectives a of a risk based and proportionate regime cannot be met whilst such a low and inflexible limit is imposed on the e-money industry.

vii. The limit is in fact so low as to make use of simplified due diligence processes non- viable, and rendering the entire legislative provision redundant.

viii. The EBA is invited to demonstrate the basis for this provision by providing empirical evidence for its adoption, and an impact

assessment on its effect on customer take-up, on product viability and friction at the point of onboarding of customers.

2. Response in relation to sectoral guidance for AIS and PIS providers.

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

General comments

PIS products enable the initiation of transactions from one regulated account holding (servicing) payment service provider to another; both of which will be regulated for prudential, conduct, financial crime risks, and will have put in place CDD, monitoring and reporting processes and controls. User funds cannot be held by a PIS provider and nor can they influence the size, frequency or timing of transactions, other than refusing to initiate a transaction entirely.

In this context, and given that the legislator has sought to bring PIS providers within the scope of obligated persons, we concur with the Guideline's provisions that such service gives rise to a low risk of money laundering, and the controls that are put in place would be calibrated accordingly.

AIS products on the other hand involve no initiation or execution of transactions, providers cannot influence any kind of activity that could give rise to money laundering and are simply independent observers of the activities undertaken by their clients. It is arguable that without specific consent and authority, AIS providers are not entitled to review their customers' data, which originate elsewhere and to do so would be an abuse of their customers' expectations of trust and confidentiality. Given that all financial services related data will have already been reviewed and be subject to monitoring and reporting obligations by the relevant originating service provider, this reinforces the absence of a nexus between an AIS service and anti-money laundering risk mitigation objectives.

Given also that AIS products encompass both regulated financial service data as well as data relating to services that are not subject to anti money laundering controls such as telecommunications and utilities related data, it would seem that requiring AIS providers to monitor such data would exceed the objectives of legislation, and to put in place Guidelines requiring it would be ultra vires, and beyond the expectations of the legislation.

Again, as the legislator has included AIS providers within the scope of obligated persons, we look to the EBA Guidelines to minimise the impact to that which is strictly necessary and which is proportionate, taking into account customers' legitimate expectations of confidentiality and trust in the AIS provider.

Any provisions that are deemed required, should be subject to a clear impact assessment and cost benefit analysis, particularly given that all payment transactions will already be subject to scrutiny by the ASPSPs that have the customer relationships for payers and payees.

Comments on Guideline 18:

Guideline 18.2 ML/TF risk is limited

Response: we concur with this assessment for the reasons stated and those set out in the general comments above.

Customer Risk Factors

18.4 a) The customer transfers funds from different payment accounts to the same payee that together, amount to a large sum without a clear economic or legitimate rationale;

Response:

I. AISPs: an AISP will have sight of the accounts of its customer held at other institutions. It will not have any means of assessing the purpose of transfers etc. and the risk of defensive reporting is such that customers could be subject to SARs when this is entirely unfounded. As the transactions were not executed or initiated by the AIS provider, they have little means of discovering the context of the transactions. Expectations of monitoring and reporting on aggregated transactions should be reconsidered and preferably removed entirely.

II. PISP: the PISP does not hold payment accounts for its payer customer, and is prohibited under Article 66(3)(g) of PSD2 from "accessing or storing any data", other than for the purpose of providing payment initiation. It is not clear how a PIS provider will be able to seek information on the purpose of transactions or store sufficient data to fulfil this obligation.

18.4 c) The customer receives funds from, or sends funds to, jurisdictions associated with higher ML/TF risk or to someone with known links to those jurisdictions.

Response: again, as the PIS/AIS provider does not hold an account for the customer, it is unable to take a view on the merits of transactions, and risks defensive reporting, as well as multiple reporting given that the relevant ASPSP ought to have made a SAR where required.

Measures

18.8 a) The customer is for PISPs: 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).

Response:

The customer, is for most current PIS business models regarded as the payee merchant. Although transactions are initiated with the payer's PSP, the PIS payment service that is

facilitated from the customer -(payer), is delivered to the payee. The payee will usually also require information confirming payment, as part of that service, in order to be able to fulfil the sale transaction.

While the PISP facilitates initiation of the payer's transactions, the party that benefits from its services, and which pays fees for the service, is the payee – merchant.

It is possible for the service to be delivered directly to the payer in different circumstances. For example, one can conceive of an App, facilitating payments on accounts belonging to the Payer on the instructions of the payer; perhaps in a semi-automated manner, choosing the most appropriate payment instrument for different payment transactions, or making periodic push payments on behalf of the payer when other criteria are fulfilled. In this case, the payment service is certainly delivered to the payer, and the PISP has not relationship with the payee.

We believe relative roles played by a PIS provider in relation to payer and payee require greater consideration and clarity, particularly in the context of AML legislation which seeks to identify and mitigate the risk of money laundering in the financial system. Guidelines could therefore refrain from addressing the issue at this stage until an appropriate discussion with stakeholders could be had.

Access to identification information

If the regulator did expect the PISP to apply CDD measures to the payer in the merchant customer model, then, given the linear nature of the transaction, it would make most sense for identification information to be made available by the payer's ASPSP through the API that is accessed by the PISP. This is not unlike transactions in other parts of the financial services sector, where brokers and other parties are involved in a single sale or payment. The different parties will share the identification, and frequently the verification information that is performed by one of the parties, usually the broker.

18.12. PISPs and AISPs should apply the CDD measures to their customers in line with Title I.

Response: (PIS) in the event that the party whose account is being accessed for initiation is regarded as the customer, then in most current business models, the occasional transaction approach will apply, as the PIPS will not have a business relationship with the payer. Their business relationship will be with the payee. It would be helpful if this is clarified.

List of EMA members as of July 2020

AAVE LIMITED
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
American Express
Azimo Limited
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Ceevo
Circle
Citadel Commerce UK Ltd
Coinbase
Contis
Corner Banca SA
Curve
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
ePayments Systems Limited
Euronet Worldwide Inc
Facebook Payments International Ltd
First Rate Exchange Services
Flex-e-card
Flywire
Gemini
GoCardless Ltd
Google Payment Ltd
IDT Financial Services Limited
Imagor SA
Intuit Inc.
Ixaris Systems Ltd
Modulr FS Europe Limited
Moneyhub Financial Technology Ltd
MuchBetter
myPOS Europe Limited
Nvayo Limited
One Money Mail Ltd
OpenPayd
Optal
Own.Solutions
Park Card Services Limited
Paybase Limited
Paydoo Payments UAB
Payoneer
PayPal Europe Ltd
Paysafe Group
Plaid
PPRO Financial Ltd
PPS
QIX Ltd
Remitly
Revolut
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Soldo Financial Services Ireland DAC
Stripe
SumUp Limited
Syspay Ltd
Token.io
Transact Payments Limited
TransferMate Global Payments
TransferWise Ltd
TrueLayer Limited
Trustly Group AB
Uber BV
Valitor
Vitesse PSP Ltd
Viva Payments SA
WEX Europe UK Limited
Wirecard AG
Wirex Limited
WorldFirst
Worldpay UK Limited
WorldRemit