Electronic Money Association
68 Square Marie-Louise
Brussels 1000, Belgium
Telephone: +44 (0) 20 8399 2066
www.e-ma.org

Raluca Pruna
Head of Unit FISMA D2 Financial Crime
European Commission, DG FISMA
Rue de Spa 2
Brussels, Belgium

18 November 2021

Dear Raluca

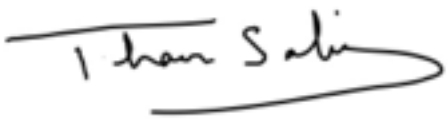
Re: ***EMA Response to the EC Consultation on a Proposal for a Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and***

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 providing online/mobile payments, card-based products, electronic vouchers, crypto asset exchanges, electronic marketplaces, merchant acquiring services and a range of other innovative payment services. Most EMA members operate across the European Union ("EU") and globally on a cross border basis. A list of current EMA members is provided at the end of this document.

We welcome the efforts of the European Commission to provide more consistency across the EU in the application of AML legislation; this will drive greater efficiencies in the operational of the AML/CTF framework, and reduce the opportunity for criminals to exploit the financial services system. However we have concerns that some elements of the Regulation are more likely to reduce efficiencies, and drive firms to allocate considerable resource towards activities that do not directly benefit the AML/CTF effort, moving the EU away from the risk-based approach, and more towards a tick-box approach to addressing AML/CTF risk.

We have set out our views below, and would be grateful for your consideration of our comments.

Yours sincerely



Thaer Sabri

Chief Executive Officer

Electronic Money Association

A - Comments on the proposed regulations on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

1. **Recital 34**

Some business models are based on the obliged entity having a business relationship with a merchant for offering payment initiation services through which the merchant gets paid for the provision of goods or services, and not with the merchant's customer, who authorises the payment initiation service to initiate a single or one-off transaction to the merchant. In such a business model, the obliged entity's customer for the purpose of AML/CFT rules is the merchant, and not the merchant's customer. Therefore, customer due diligence obligations should be applied by the obliged entity vis-a-vis the merchant.

Whilst the EMA welcomes the clear guidance on the roles played by a Payment Initiation Service provider in relation to payer and payee, we would also make the following points:

- It is our view that the inclusion of PIS providers within the scope of obligated entities is disproportionate to the risks that could be mitigated by any PISP. PISPs essentially provide technical services to assist a payer in making payments and a payee in ensuring that they receive such payments. Both payer and payee retain their existing payment service providers (PSP), and could not in fact benefit from the services of a PISP unless they enter into a business relationship with their own PSP – (referred to in PSD2 as an ASPSP).
- The PISP is not in the flow of funds and does not introduce any additional parties into the payment transaction; payment continues to be undertaken directly from payer to payee through their existing PSPs. The PISP simply provides the means for the payment to be arranged by the payer by facilitating the submission of data and assisting the payer in initiating the payment.
- The scope of obligated entities under the FATF Recommendations falls short of the activity undertaken by PISPs. The FATF, when capturing PSPs, does so by including 'Financial Institutions' within its scope. The latter are defined as firms that undertake a number of activities, including:
    - Money or value transfer services. (It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds.)
    - Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).

  There are no money or value transfer services offered, nor can the technical services that are delivered be considered 'management of a means of payment'. There is little reason therefore to extend the EU AML regime to PISPs. There is similarly little risk that such an approach would fall short of FATF obligations.
- It should be noted that both payer and payee are subject to CDD processes by their respective PSPs, and that the payment transaction will be visible to both payer and payee PSPs or ASPSPs, and can therefore be monitored and reported where that is appropriate. Regulating a PISP for AML/CTF is therefore duplicative of the CDD, monitoring, record keeping, reporting and compliance obligations that would result when applying the AML regime to PISPs.

We therefore suggest that the legislator considers the exclusion of PISPs from the scope of obligated entities; enabling the removal of regulation that offers little benefit and adds

little that is not already provided by the already regulated PSPs of payers and payees. We urge the legislator to remove PISPs from the scope of obligated entities.

We also believe the arguments made above apply even more strongly to AISPs, which do not conduct any payment transactions, but merely offer data services to users, based on their existing transactional information. It is difficult to identify a rationale for the inclusion of such services within the scope of AML regulation. There are no other data service providers captured within the scope of the legislation, and inclusion of AISPs would be highly anomalous. There are also no equivalent categories of obligated entities in the FATF Recommendations that would capture such activities. It would therefore be disproportionate to extend the scope of AML regulation to AISPs, and it also follows that excluding AIS providers would not give rise to a risk of non-compliance with FATF obligations. There is conversely a real risk to AIS businesses themselves, that users, recognising that their personal data is being monitored, analysed and then potentially reported, would also regard this as disproportionate and unwarranted. There would then be a good likelihood of users deciding to refrain from taking up such services in their entirety. AML legislation applied to AIS providers has the capacity to cool the market off, for such services and to undermine the open banking and open data project at its inception. We urge legislators to reconsider the inclusion of AISPs within the scope of AML legislation.

2. Article 2(25)

The current definition of a Politically Exposed Person in 4MLD provides at Article 3(9) 4MLD: '*…No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials.'* This text has been removed from the text in the current proposal.

We welcome the fact that the lists are now exhaustive, but request that the clarification about middle-ranking or more junior officials be reinstated. If civil servants fell under the definition, this would increase the number of PEPs significantly.

3. Article 7(2)(b) and (c)

The policies, controls and procedures referred to in paragraph 1 shall include: *(…)*
(b) policies, controls and procedures to identify, scrutinise and manage business relationships or occasional transactions that pose a higher or lower money laundering and terrorist financing risk. *(c) an independent audit function to test the internal policies, controls and procedures referred to in point (a);*

We would appreciate further clarity as to whether Art. 7(2)(b) refers to classification of customers in order to facilitate SDD and EDD, or whether this is a more general obligation that has been introduced. If so, we would welcome further clarity or a rationale on the purpose of the classification and scrutiny.

Art. 7(2)(c) mandates the establishment of proportionate policies/controls/procedures for an independent audit ("IA") function to test the internal policies, controls and procedures. The requirement to introduce Independent audit in all cases (in contrast to the current situation in 4MLD 'where appropriate with regard to the size and nature of the business') is disproportionate for a large number of obliged entities, and will introduce significant

administrative, operational and financial burdens on smaller firms. We request the reinstatement of the proportionality condition for the undertaking of Independent audits.

4. Article 9(3)

(...)
An obliged entity that is part of a group may appoint as its compliance officer an individual who performs that function in another entity within that group.

We welcome the allowance to appoint the compliance officer at group level. In addition, we consider that, given the international dimension of financial services and the use of outsourced service providers, it is operationally effective for the location of the AML/CFT compliance officer to be as close to the centralised operations as possible. This may be in the country of establishment, or may be elsewhere.

5. Article 11(1)

Any employee of an obliged entity entrusted with tasks related to the obliged entity's compliance with this Regulation and Regulation [...] shall undergo an assessment approved by the compliance officer of:
(a) individual skills, knowledge and expertise to carry out their functions effectively;
(b) good repute, honesty and integrity.

The article has been drafted very broadly, and could better specify the personal data that firms must collect in order to establish good repute, honesty and integrity, or provide that this is undertaken on a risk-sensitive basis. There is then the consequent issue of the range of employees that must be subject to such an assessment. We suggest that the text clarifies that such an assessment does not extend beyond those with specific responsibilities under AML regulation i.e., excluding customer service, for example.

6. Article 13(3)

(...) AMLA shall develop draft regulatory technical standards and submit them to the Commission for adoption. Those draft regulatory technical standards shall specify the minimum requirements of group-wide policies, including minimum standards for information sharing within the group, the role and responsibilities of parent undertakings that are not themselves obliged entities with respect to ensuring group-wide compliance with AML/CFT requirements (...)

In relation to the proposed RTS specifying the minimum requirements of group-wide policies to be issued by AMLA, care should be taken to avoid the impression that AMLA may impose requirements on parent companies that are not themselves regulated. While these companies may play a role in overseeing certain aspects of the group's AML compliance, responsibility for such compliance should solely lie with the regulated entities of the group.

7. Article 15

Application of customer due diligence
1. Obliged entities shall apply customer due diligence measures in any of the following circumstances:

(...)
(b) when involved in or carrying out an occasional transaction that amounts to EUR 10 000 or more, or the equivalent in national currency, whether that transaction is carried out in a single operation or through linked transactions, or a lower threshold laid down pursuant to paragraph 5;
2. In addition to the circumstances referred to in paragraph 1, credit and financial institutions and crypto-asset service providers shall apply customer due diligence when either initiating or executing an occasional transaction that constitutes a transfer of funds as defined in (...)

We would welcome further clarification around the term 'involved in' in Art. 15(1(b), so as to avoid misinterpretation. It is unclear, for example, whether this phrase is designed to capture the services provided by Payment Initiation Service Providers (PISPs). It is also unclear why the transfer of funds EUR 1,000 limit in Art. 15(2) is phrased distinctly, using 'initiating or executing' rather than 'involved in or carrying out'. We propose that both instances are restricted to 'executing' of transactions, as other instances would simply be duplication of CDD undertaken by the entity executing the transaction.

8. Removal of the e-money-specific exemption from CDD

It is unclear why the exemption from CDD for certain low-value e-money instruments has been removed. The exemption allows CDD to be postponed until the customer has used the product to an extent that justifies undertaking due diligence, both from the perspective of risk and the cost of undertaking CDD. Without these thresholds, the cost of undertaking CDD at the outset[1] would be prohibitive given the narrow profit margins that such restricted products have. Currently, a significant proportion of e-money cards and vouchers issued in the EEA benefit from the e-money exemption under the 4MLD; it is vital for the industry that this allowance should continue, and the removal of the exemption will impact both issuers and EU consumers alike.

We are further surprised that industry was not consulted prior to proposed change, nor was there a request for an impact assessment. Given the significant restrictions that were placed on the use of the exemptions in 5MLD in order to limit any risks from the exemption (for example, person-to-person transfers are prohibited and transactions online are limited to EUR50 in value and transaction monitoring required in Article 21 mitigates any residual risk), it is also hard to understand the rationale for the removal of the exemption so soon afterwards.

We would furthermore like to stress that users of e-money have legitimate needs for a private low-value means of payment. This was highlighted in the recent ECB consultation on the issues most important in civil society when considering the use of CBDCs. Privacy was three times more valued than any other attribute. Restricting industry's ability to offer products to users in this context is surprising.

Compared to cash, e-money offers significant visibility of transactions and consequently generates information that can be made available to law enforcement. By removing CDD-

[1] The cost of verification is in the region of EUR 2 to EUR 8; making a EUR 100 prepaid card (or lower) non-viable as a payment product when compared to credit or debit cards. Merchants are typically charged 1-2% of transaction values for debit or credit card acceptance, and so are unlikely to be willing to accept charges that would need to be in excess of 5% in order to accommodate CDD related costs.

related barriers to the take-up of e-money by consumers as well as retailers, the displacement of cash activity within the economy is promoted. The displacement of cash is both a general good and a specific objective of the FATF.

E-money products also play an important role in financial inclusion by providing secure access to online commerce to persons who are not able to gain such access through traditional payment products.[2] Higher friction for users of low value e-money products immediately reduces take-up and restricts financial inclusion for those who do not have access to bank or credit card facilities.[3] Given the prevalence of cheaper products and services online, this is particularly significant for those whose financial exclusion goes hand in hand with limited means. E-money cards are mostly sold in retail locations, and both users and distributor retailers have indicated that identification and verification of such low value products is impractical and cumbersome.

In summary, the e-money products that benefit from the existing exemption from CDD are limited in functionality, limited in the value of funds that can be transacted, and offer a number of advantages for both users and law enforcement. There has not, to our knowledge, been any systemic or significant vulnerabilities that have enabled the abuse of these products for either money laundering or terrorist financing, and we think it is therefore disproportionate to limit legitimate use of these products. Instead, we support the holistic approach taken by the European Supervisory Authorities to identify risk factors relevant to e-money products and to seek to mitigate them.

We suggest that the exemption is reinstated, or material evidence and rationale for its removal produced.

9. Article 16(2)

Obliged entities shall determine the extent of the measures referred to in paragraph 1 on the basis of an individual analysis of the risks of money laundering and terrorist financing having regard to the specific characteristics of the client and of the business relationship or occasional transaction (...)

It is not practicable to carry out an individual risk analysis for each customer and beneficial owner, as appears to be required by Art. 16(2). Provision should be made for a risk-based approach that allows the obliged entity to determine the risk of customers at the level of

[2] The FATF has been critical of a one-fits-all approach to CDD requirements in its 2013 guidance Anti-Money Laundering and Terrorist Financing and Financial Inclusion: 'While the 2003 FATF Recommendations were also intended to encourage countries to apply an RBA, and did impose certain RBA related obligations, a review of the results of countries' assessments carried out between 2005 and 2011 (among the FATF and the FSRBs community) shows that very few countries took full advantage of this flexibility. Rather, most countries have introduced a uniform approach with the same AML/CFT requirements applicable to all financial institutions, clients, products and services. This may have hampered financial inclusion efforts of financial providers. At the customer level, customers who conduct limited and small value (potentially lower risk) financial transactions must often meet the same customer due diligence requirements as higher risk customers who frequently conduct large transactions.'

[3] Our experience is that the take-up of products drops in excess of 50% where CDD information is requested.

the product proposition where appropriate, taking into account general features of the relationship and any controls applied.

10. Article 18(1) and (2)

With the exception of cases of lower risk to which measures under Section 3 apply and irrespective of the application of additional measures in cases of higher risk under Section 4 obliged entities shall obtain at least the following information in order to identify the customer and the person acting on their behalf:
(a) for a natural person:
(i) the forename and surname;
(ii) place and date of birth;
(iii) nationality or nationalities, or statelessness and refugee or subsidiary protection status where applicable, and the national identification number, where applicable;
(iv) the usual place of residence or, if there is no fixed residential address with legitimate residence in the Union, the postal address at which the natural person can be reached and, where possible, the occupation, profession, or employment status and the tax identification number;
(b) for a legal entity:
(i) legal form and name of the legal entity;
(ii) address of the registered or official office and, if different, the principal place of business, and the country of incorporation;
(iii) the names of the legal representatives as well as, where available, the registration number, the tax identification number and the Legal Entity Identifier. Obliged entities shall also verify that the legal entity has activities on the basis of accounting documents for the latest financial year or other relevant information;
(...)
(d) for other organisations that have legal capacity under national law: (i) name, address of the registered office or equivalent; (ii) names of the persons empowered to represent the organisation as well as, where applicable, legal form, tax identification number, register number, Legal Entity Identifier and deeds of association or equivalent.

The specification of an extensive list of elements of identity moves the AML framework away from a risk-based approach to the prevention of ML/TF and towards one that is tick-box in nature. It is, for example, unclear why the nationality and profession of a customer would need to be obtained for the purchase of a low-value payment instrument such as a prepaid card. Equally, a tax ID number may be useful where savings or investments are concerned, but is hardly proportionate to the risk of payment products intended for the purchase of goods or services. We furthermore note that tax ID numbers are not a consistent form of identification across EU member states. It is also difficult to envisage how profession, employment status or tax ID numbers can be verified other than by obtaining physical documents, which undermines the progress made in adapting the legislation to the current trend towards online means of verification (also see our comments on the remainder of article 18 below).

Furthermore, the extension of the number of identity elements increases the risk of identity theft and related fraud, and is contrary to the principles of purpose limitation and data minimisation. The holding of larger data sets without a meaningful purpose increases the risk that obliged entities will be targets of cyber attacks. In order to help combat financial

and identity-related crime more generally, it would be better to implement data minimisation principles and ensure only information that is required is held.

We would also welcome clarity regarding the following aspects of the list of identity elements:

- The identity requirements apply 'with the exception of cases of lower risk to which measures under Section 3 apply.' However, the SDD provisions in Section 3 do not seem to permit a reduction or variation of the elements of identity verified.
- 'Where possible' in Art. 18(1)(a)(iv): Does this refer to physical constraints on systems, the existence of a profession, or the customer's willingness to disclose this? More definitive wording is proposed, but the elements should not be mandatory as they are not relevant in all circumstances and to all products.
- 'Legal representatives' in Art. 18(1)(b)(iii): Does this refer to Directors or legal professionals?
- The meaning of 'where applicable' in Art. 18(1)(d) is unclear.
- It is furthermore unclear why, when identifying the beneficial owner (who is defined as a natural person), the identity of a legal entity must also be verified under Art. 18(2), and which legal entity is being referred to.

11. Article 18(4)

> *Obliged entities shall obtain the information, documents and data necessary for the verification of the customer and beneficial owner identity through either of the following:*
> *(a) the submission of the identity document, passport or equivalent and the acquisition of information from reliable and independent sources, whether accessed directly or provided by the customer;*
> *(b) the use of electronic identification means and relevant trust services as set out in Regulation (EU) 910/2014.*

There is some uncertainty as to the requirements in provision 18(4)(a); if this requires the submission of identity documents in every case, then this is neither risk-based nor in keeping with modern means of verifying identity using evolving technology. If, however, this is an alternative to the second part of the sentence allowing for the acquisition of information from a reliable and independent source as an alternative, then this is more workable. In the latter case, we strongly suggest replacing 'and, with 'or' to make it clear that these are alternatives.

We have the same point to make for part 18(4)(b) where electronic identification means should be an alternative to trust services set out in Regulation EU 910/2014. In this case, 'and' should again be replaced with 'or' for clarity. If on the other hand, electronic identification is only permissible in the context of the eIDAS Regulation, then this is overly restrictive and will result in most means of verification being non permissible.

More generally, we would like to reiterate the importance of a risk-based approach to CDD, which is essential, given the significant differences between financial sector business models, for instance in relation to the transaction volume, frequency and scalability. Enhanced up-front verification procedures that require potentially lengthy and complex procedures may lead to financial exclusion and may also deter customers from using some

products altogether. This may push customers towards an increased usage of cash or informal value transfer systems, which pose higher ML/TF risks.

High relative on-boarding/compliance costs would furthermore obstruct competition and innovation in the market, and higher operational costs will ultimately be borne by the customer, slowing the growth of business and potentially affecting the under-banked hardest.

12. Article 20

Identification of the purpose and intended nature of a business relationship or occasional transaction Before entering into a business relationship or performing an occasional transaction, an obliged entity shall obtain at least the following information in order to understand its purpose and intended nature:
(a) the purpose of the envisaged account, transaction or business relationship;
(b) the estimated amount and economic rationale of the envisaged transactions or activities;
(c) the source of funds;
(d) the destination of funds.

The requirements are onerous particularly for small-value and limited purpose instruments. Requiring information about the source of funds for a product that involves an aggregate turnover of EUR 1,000 over the course of a month, or for the purchase of a EUR 50 prepaid card bought in a retail outlet, is not practicable nor risk-sensitive.

The 'destination of funds' requirement is unclear. Is it envisaged that when opening a payment account, customers are required to specify where they intend to spend/transfer funds from the account, possibly over many years of usage? This would hardly be feasible. In any case, payee/beneficiary information is already captured as part of the requirements under the Funds Transfer Regulation.

Equally, the 'estimated amount' may be possible to establish for occasional transactions but not for longer-term business relationships. We also note that it could be difficult for firms to identify and determine an 'economic rationale' for all new customers, particularly if the payment instrument is for general payment purposes online.

Where SDD products are concerned, the possibility to reduce the amount of information collected to identify the purpose and intended nature of the business relationship or infer it from the type of transactions or business relationship established is welcomed. However, this should be available not only in SDD circumstances, but in all circumstances where the purpose and intended nature of the business relationship is clear from the product proposition.

13. Article 21(3)

In addition to the requirements set out in paragraph 2, obliged entities shall review and, where relevant, update the customer information where: (...)
(c) they become aware of a relevant fact which pertains to the customer

It is unclear what is meant by 'relevant fact which pertains to the customer' in Art. 21(3)(c).

14. Article 22 on Regulatory Technical Standards developed by AMLA on the information necessary for the performance of CDD

We suggest that, in line with our comments above, AMLA should outline a risk-based approach in their RTS on CDD information and not seek to provide specific requirements. The risk-based approach to CDD is essential, given the significant differences between financial sector business models, for instance in relation to the transaction volume, frequency and scalability. Enhanced up-front verification procedures that require potentially lengthy and complex procedures may lead to financial exclusion, to increased costs and may also deter customers from using some products altogether. This may push customers towards an increased usage of cash or informal value transfer systems, which pose higher ML/TF risks.

15. Article 23 on the identification of third countries with strategic deficiencies refers to natural or legal persons 'from that country'

This reference appears to have a broad scope and could have a wider impact than intended. For example, it could include residents in EU member states who originate from a third country.

The approach of 4MLD Article 18 and in other parts of the AML Regulation, which refer to natural persons or legal entities *established* in third countries, is preferable.

16. Article 24

> *Identification of third countries with compliance weaknesses in their national AML/CFT regimes*
> *1.Third countries with compliance weaknesses in their national AML/CFT regimes shall be identified by the Commission.*
> *…*
> *4.The delegated act referred to in paragraph 2 shall identify the specific enhanced due diligence measures among those listed in Article 28(4), points (a) to (g), that obliged entities shall apply to mitigate risks related to business relationships or occasional transactions involving natural or legal persons from that third country.*

The proposal to develop a delegated act that will set out specific EDD measures that obliged entities must apply in order to mitigate risks associated with 'persons from that third country' with compliance weaknesses in their national AML/CFT regimes appears to be overly prescriptive.

Furthermore, the reference to 'customers from that third country' is discriminatory and may possibly be in breach of Article 14 of the European Convention on Human Rights by discriminating against citizens based on their ethnic origin. We suspect this is not the intended meaning and ask that this is remedied.

Enhanced up-front verification procedures that require potentially lengthy and complex procedures may lead to financial exclusion and may also deter customers from using some

products altogether. This may push customers towards an increased usage of cash or informal value transfer systems, which pose higher ML/TF risks.

17. Article 26(1)

> *(...) AMLA shall adopt guidelines defining the money laundering and terrorist financing trends, risks and methods involving any geographical area outside the Union to which obliged entities are exposed (...).*

This appears to be an additional layer over and above the requirements that apply in relation to third countries as defined in the Regulation, and could result in yet another source of EDD obligations. In line with existing EBA Guidance, we consider that such risks should be addressed as part of a risk-based assessment, and not by prescriptive guidance.

18. Article 27

> *Simplified customer due diligence measures*
> *1. Where, taking into account the risk factors set out in Annexes II and III, the business relationship or transaction present a low degree of risk, obliged entities may apply the following simplified customer due diligence measures:*
> *(a) verify the identity of the customer and the beneficial owner after the establishment of the business relationship, provided that the specific lower risk identified justified such postponement, but in any case no later than 30 days of the relationship being established;*
> *(...)*
> *3. For the purpose of applying simplified due diligence measures referred to in paragraph 1, point (a), obliged entities shall adopt risk management procedures with respect to the conditions under which they can provide services or perform transactions for a customer prior to the verification taking place, including by limiting the amount, number or types of transactions that can be performed or by monitoring transactions to ensure that they are in line with the expected norms for the business relationship at hand.*

In Article 27(1) first paragraph, 'low' should be replaced with 'lower'. 'Low' implies the existence of an absolute standard applicable to all obligated entities, while 'lower' allows for entities to take a view on risk in the context of their products and services. 'Lower' is also the term used in Article 27(1)(a).

The 30-day limit appears arbitrary and is not supported by low-risk business propositions. For example, a low-value e-money instrument for purchasing goods or services does not increase in risk because the customer holds it for more than 30 days, or even 60 days. Re-load and spending may occur in longer intervals, and a small balance may remain over time, which the customer does not wish to spend or withdraw but which would not warrant the application of CDD.

It is also questionable why a time limit has been adopted whilst at the same time, transaction limits must be put in place under Article 27(3). A more workable approach would be to require such transaction limits in order to ensure a lower risk without an

additional time limit on postponing verification. This approach is currently permitted under EBA and Irish guidance,[4] but has not been reflected here.

Notably absent from the list of possible SDD measures is the reduction in the amount of information (even though Article 18 applies 'with the exception of cases of lower risk to which measures under Section 3 apply') or the use of different kinds of information, for identification and verification purposes (also see our comments on Article 18). Providing such an option is important to ensure that lower risk business propositions are not made non-feasible by the cost of the CDD measures required under Article 18.

There are also practices that have been used for some 20 years and which have been subject to repeated FATF mutual evaluation assessments, such as establishing that CDD has been undertaken by the funding instrument financial institution, as a means to implement SDD. This has been an effective means of undertaking SDD and has been a key component of customer journeys for a significant length of time. Legislation should not exclude its use by restricting the means of undertaking CDD.

19. Article 32

1. In addition to the customer due diligence measures laid down in Article 16, obliged entities shall have in place appropriate risk management systems, including risk-based procedures, to determine whether the customer or the beneficial owner of the customer is a politically exposed person.
2. With respect to transactions or business relationships with politically exposed persons, obliged entities shall apply the following measures:
(a) obtain senior management approval for establishing or continuing business relationships with politically exposed persons;
(b) take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with politically exposed persons;
(c) conduct enhanced, ongoing monitoring of those business relationships.

We welcome the fact that, as under 4MLD, the requirement to identify PEPs is itself risk-based (Article 32(1)). This allows firms with small-value payment products that offer limited potential for abuse to set risk-based thresholds for PEP identification.

In relation to Article 32(2), it was previously clear that the source of wealth/funds only needed to be obtained for transactions within a business relationship with a PEP. Now, there seems to be a requirement to obtain information on the source of wealth/funds also for transactions outside of a business relationship. We would welcome further clarity in this regard.

20. Articles 35 and 36

Measures towards persons who cease to be politically exposed persons
1. Where a politically exposed person is no longer entrusted with a prominent public function by the Union, a Member State, third country or an international organisation,

[4] Paragraph 4.41(ii) of the EBA's 'Guidelines on Money Laundering and Terrorist Financing Risk Factors' (March 2021); paragraph 5.4.1 of the CBI's 'Anti-Money Laundering and Countering the Financing of Terrorism Guidelines for the Financial Sector' (June 2021).

obliged entities shall take into account the continuing risk posed by that person in their assessment of money laundering and terrorist financing risks in accordance with Article 16.

2. Obliged entities shall apply one or more of the measures referred to in Article 28(4) to mitigate the risks posed by the business relationship, until such time as that person is deemed to pose no further risk, but in any case for not less than 12 months following the time when the individual is no longer entrusted with a prominent public function.

3. The obligation referred to in paragraph 2 shall apply accordingly where an obliged entity enters into a business relationship with a person who in the past was entrusted with a prominent public function by the Union, a Member State, third country or an international organisation.

Article 36 Family members and close associates of politically exposed persons

The measures referred to in Articles 32, 34 and 35 shall also apply to family members or persons known to be close associates of politically exposed persons.

The extension of EDD measures to persons who were PEPs in the past is likely to constitute a significant compliance burden. Persons who have been out of office for 12 months should no longer be regarded as PEPs.

In addition, the entirety of requirements relating to persons who are no longer PEPs (whether they ceased to be so before or after the start of the business relationship) have also been applied to family members or close associates of PEPs, increasing the compliance burden. This could increase the size of the PEP dataset by several orders of magnitude and make the possibility of non compliance more likely. We suggest a time limit be introduced, rather than an open ended retrospective obligation.

Customers will need to disclose details about past functions and relationships, without a time limit. This may reduce the number of financial services products available for PEPs, and will affect their entire families and network of friends.

21. Article 40(1) and (2)

1. Obliged Obliged entities may outsource tasks deriving from requirements under this Regulation for the purpose of performing customer due diligence to an agent or external service provider, whether a natural or legal person, with the exception of natural or legal persons residing or established in third countries identified pursuant to Section 2 of this Chapter.

2. (...) The following tasks shall not be outsourced under any circumstances:
(a) the approval of the obliged entity's risk assessment;
(b) the internal controls in place pursuant to Article 7;
(c) the drawing up and approval of the obliged entity's policies, controls and procedures to comply with the requirements of this Regulation;
(d) the attribution of a risk profile to a prospective client and the entering into a business relationship with that client;

(e) the identification of criteria for the detection of suspicious or unusual transactions and activities;
(f) the reporting of suspicious activities or threshold-based declarations to the FIU pursuant to Article 50

It is unclear what is meant by 'external service providers:' We assume this category does not include group companies, and we assume that the list under paragraph 2 does not relate to the operational activity but rather to the decision making. Otherwise, the application of paragraph 2 of this Article would lead to significant challenges for regulated entities. For example, the operational activity of approving the obliged entity's risk assessment is often done by an entity within the group. If it were prohibited for a group entity to conduct this activity, this would be problematic.

Article 40(2)(b) prohibits the outsourcing of all internal controls under Art. 7. The scope of these internal controls is very wide and encompasses all internal controls including CDD, record keeping, ongoing monitoring, training, etc. We consider that the intention is not to prohibit the outsourcing of all the activities under Article 7 outright and suggest that the provision either be deleted or be made more specific.

Under Article 40(2)(c), firms should be allowed to outsource the 'drawing up' of policies, controls and procedures provided these are approved internally. Updates could, for example, be completed by other group entities handling operational tasks or consultancies ahead of approval by the obliged entity. Processes are often drafted by customer-facing staff, e.g., at group level, as they are best informed about customer and operational needs. It would not be sensible to require all processes and policies to be designed and updated at the head office; they should be allowed to be drafted by other entities, e.g., centralised operations entities.

Article 40(2)(d) should be clarified to say that it refers to the underlying concept rather than the operational steps undertaken during the onboarding of a customer. The actual attribution of a risk profile is in many cases an automated process, which could also be handled by tools outsourced to a third party. The underlying design and approval of the risk profiles can be completed by obliged entities, but the execution of the tasks by expert staff based on predefined policies and processes should not have to be completed in-house.

22. Article 50(1)

Reporting of suspicious transactions
1. Obliged entities shall report to the FIU all suspicious transactions, including attempted transactions. Obliged entities, and, where applicable, their directors and employees, shall cooperate fully by promptly:
(a) reporting to the FIU, on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing, and by responding to requests by the FIU for additional information in such cases;
(b) providing the FIU directly, at its request, with all necessary information.

For the purposes of points (a) and (b), obliged entities shall reply to a request for information by the FIU within 5 days. In justified and urgent cases, FIUs shall be able to shorten such a deadline to 24 hours.

The EMA and EMA members actively cooperate with law enforcement and FIUs in all EU member states and regularly respond to data requests and notices issued in relation to ongoing investigations. However, providing information to the FIU within 24 hours should only be required in the most extreme of circumstances, as this is otherwise not feasible at scale. These circumstances should furthermore be defined in advance. Under Article 39, obliged entities that are relied on are awarded five days to provide CDD information. We suggest that a similar time frame (if any) also applies to this obligation to provide information to the FIU.

23. Article 55

To the extent that it is strictly necessary for the purposes of preventing ML/TF, obliged entities may process special categories of personal data and personal data relating to criminal convictions and offences subject to certain safeguards.

Under the GDPR, processing special category data (i.e., sensitive data such as racial or ethnic origin, political opinions, religious beliefs, etc.) is prohibited [GDPR 9(1)] unless an exception applies (such as the processing is necessary for reasons of substantial public interest) [GDPR 9(2)(g)].A

This Article appears very broad, and does not precisely limit the scope of the data processing by obliged entities to the extent that it is necessary and proportionate for the purposes of preventing ML/TF. It should be drafted more clearly and set out the types of data that will be processed by obliged entities when they carry out certain measures (e.g., CDD, reporting SARs, etc.) Processing of personal data relating to sexual orientation or ethnic origin should not be allowed.

24. Article 58

Anonymous accounts and bearer shares and bearer share warrants
1. Credit institutions, financial institutions and crypto-asset service providers shall be prohibited from keeping anonymous accounts, anonymous passbooks, anonymous safe-deposit boxes or anonymous crypto-asset wallets as well as any account otherwise allowing for the anonymisation of the customer account holder.

It is unclear what the phrase ‘as well as any account otherwise allowing for the anonymisation of the customer account holder’ is aimed at, and whether this applies only/not to crypto-asset wallets or all types of accounts.

List of EMA members as of November 2021

AAVE LIMITED
Account Technologies
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
American Express
ArcaPay Ltd
Azimo Limited
Bitpanda Payments GmbH
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Circle
Citadel Commerce UK Ltd
Contis
Corner Banca SA
Crosscard S.A.
Crypto.com
Curve
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
emerchantpay Group Ltd
ePayments Systems Limited
Etsy Ireland UC
Euronet Worldwide Inc
Facebook Payments International Ltd
Financial House Limited
First Rate Exchange Services
FIS
Flex-e-card
Flywire
Gemini
Global Currency Exchange Network Limited
Globepay Limited
GoCardless Ltd
Google Payment Ltd
HUBUC
IDT Financial Services Limited
Imagor SA
Ixaris Systems Ltd
Modulr FS Europe Limited
MONAVATE
Moneyhub Financial Technology Ltd
Moorwand
MuchBetter
myPOS Europe Limited
OFX
OKTO
One Money Mail Ltd
OpenPayd
Own.Solutions
Oxygen
Park Card Services Limited
Paydoo Payments UAB
Paymentsense Limited
Payoneer Europe Limited
PayPal Europe Ltd
Paysafe Group
Plaid
PPRO Financial Ltd
PPS
Remitly
Revolut
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Snowy Pay Ltd.
Soldo Financial Services Ireland DAC
Square
Stripe
SumUp Limited
Syspay Ltd
Transact Payments Limited
TransferMate Global Payments
TrueLayer Limited
Trustly Group AB
Uber BV
Vitesse PSP Ltd
Viva Payments SA
Vivid Money Limited
Weavr Limited
WEX Europe UK Limited
Wirex Limited
Wise
WorldFirst
WorldRemit LTD