



**Electronic Money Association**

68 Square Marie-Louise

Brussels 1000

Belgium

[www.e-ma.org](http://www.e-ma.org)

Carolin Gardner  
Head of Unit, AML-CFT  
European Banking Authority  
Tour Europlaza 20  
Avenue André Prothin,  
92400 Courbevoie France

6 June 2025

Dear Carolin

**Re: EMA response to [Consultation Paper on Response to Call for Advice new AMLA mandates](#)**

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide, providing online payments, card-based products, electronic vouchers, and mobile payment instruments. Most members operate across the EU, most frequently on a cross-border basis. A list of current EMA members is provided at the end of this document.

I would be grateful for your consideration of our comments and proposals.

Yours sincerely,

A handwritten signature in dark ink, which appears to read 'Thaer Sabri', is positioned above a long, horizontal, slightly wavy line that serves as a decorative flourish or underline.

Dr Thaer Sabri  
Chief Executive Officer  
Electronic Money Association

## **EMA Response to the Draft RTS on the risk assessment for the purpose of selection of credit institutions, financial institutions and groups of credit and financial institutions for direct supervision under Article 12(7) of the AMLAR**

### **Question 1**

**Do you agree with the thresholds provided in Article 1 of the draft RTS and their value? If you do not agree, which thresholds to assess the materiality of the activities exercised under the freedom to provide services should the EBA propose instead? Please explain your rationale and provide evidence of the impact the EBA's proposal and your proposal would have.**

### **EMA Comment**

While the EMA supports the principle of using thresholds to assess the materiality of activities conducted under the freedom to provide services, we believe the thresholds proposed in Article 1 of the draft RTS require refinement to ensure they are proportionate, clear, and reflective of varying business models and risk profiles across the market. We do not agree with the current thresholds set out in Article 1 and believe that they are set too low.

Additionally, the EMA would like to stress the importance of using clearly defined terms for the data to be collected in the context of materiality threshold assessments, particularly regarding customer and transaction classification. Ambiguities in these definitions can lead to inconsistent interpretations and undermine the reliability of risk assessments. We therefore encourage the development of detailed guidance on each data point to support obliged entities in establishing accurate and consistent reporting practices

- **Customer number threshold Article 1(1)(a)**

The proposed 20,000-customer threshold represents less than 1% of the population in nearly all EU Member States, with the exception of smaller jurisdictions such as Malta (3.8%), Latvia (1.05%), Estonia (1.54%), Cyprus (1.67%), and Luxembourg (3.13%). This suggests that the threshold is not aligned with population size or market relevance. Many obliged entities can easily exceed this number due to the nature of cross-border service provision and passporting rights within the EU. Such a low threshold risks overwhelming AMLA's supervisory capacity and diluting its focus on genuinely high-risk entities.

Moreover, the term "customers" is not clearly defined, which creates uncertainty in interpreting the threshold. It is unclear whether the threshold refers only to active customers, or whether it also includes inactive accounts, or customers pending off-boarding. As the customer count is central to the materiality assessment, a definition is necessary. Relying on the total number of customers without distinguishing between active and inactive may not accurately reflect the actual level of activity, associated risk, and the materiality of cross-border operations.

We suggest modifying the customer number threshold in accordance with a risk-based approach, to only include active customers, particularly those who have conducted at least one transaction in the previous year. In business models where a relatively small number of customers can generate high transaction volumes, such as B2B services, this would provide a more accurate representation of the true scale and risk profile of cross-border operations.

This adjustment is both possible and significant given that data on active customers is already anticipated to be gathered under Annex I, Section B. This would also assist in the prevention of distorted results where legacy or defunct accounts exaggerate customer numbers without increasing the exposure to ML/TF risk.

The EMA recommends increasing the customer threshold to at least 100.000 active customers in each of 6 EU member states.

- **Transaction value threshold Article I(1)(b)**

While the transaction volume threshold generally serves as a useful indicator of material activity, the proposed threshold of EUR 50 million euro threshold is too low. It can be reached quickly by a small number of high-net-worth clients, even in low-risk business models, and does not accurately reflect material risk or operational scale.

In addition to the threshold being low, we note that key terms such as “transaction” and “nature of transaction” are not clearly defined. The lack of clarity creates uncertainty around what types of activities should be included in calculation. . The EMA recommends incorporating a breakdown by transaction type such as for example card payment, cash withdrawals, or bank transfers, as each carries different risk levels, especially in relation to AML/CFT considerations. To enhance proportionality, and ensure the thresholds better reflect the actual risk, we propose that the EBA consider thresholds account for:

- the activity level of customers (active vs inactive);
- the type of client (retail vs institutional);
- the nature of transactions (categorized by ML/TF risk level, and specifying whether, for example, issuance of e-money/EMT included); and
- the business model and sector-specific risks.

## **Question 2**

**What is your view on the possibility to lower the value of the thresholds that are set in article I of the draft RTS? What would be the possible impact of doing so? Please provide evidence.**

### **EMA Comment**

The EMA does not support lowering the thresholds set out in Article I. We believe the current thresholds are too low and lowering them even more would only broaden the scope of institutions subject to the materiality assessment and associated costs, including many that do not necessarily pose a high level of ML/TF risk, thereby reducing proportionality and potentially diverting supervisory focus from higher-risk areas.

### Question 3

**Do you agree on having a single threshold on the number of customers, irrespective of whether they are retail or institutional customers? Alternatively, do you think a distinction should be made between these two categories? Please explain the rationale and provide evidence to support your view.**

#### EMA Comment

The EMA supports distinguishing between retail and institutional customers, given the significant differences in risk profiles and operational realities, and therefore suggests reevaluating the application of a single customer threshold, as it may not accurately reflect the true nature and scale of AML/CFT risks.

We recommend considering a wide range of factors, including customer volume, onboarding process, the nature and purpose of business relationship, transaction frequency and patterns, sector classification, ownership structure, availability of due diligence information, exposure to vulnerabilities such as politically exposed persons or sanctions risks.

A firm providing services to a small number of institutional or high-risk business clients could pose a substantially greater risk than one with a larger retail customer base. However, under the current 20,000-customer threshold, such firms may not meet the materiality criteria. In contrast, businesses with large retail customer bases may exceed this threshold even if their overall risk exposure differs substantially.

Applying a single threshold across diverse client segments may result in disproportionate outcomes, underestimating risks in certain high-risk business models and overemphasising lower-risk retail businesses that exceed the numerical limit. We therefore recommend adopting a distinct approach with separate standards for retail and institutional customers. This would allow supervisors to better identify material activities based on underlying risks, hence improving supervisory proportionality.

### Question 4

**Do you agree that the methodology for selection provided in this RTS builds on the methodology laid down in the RTS under article 40(2)? If you do not agree, please**

**provide your rationale and evidence of the impact the EBA's proposal and your proposal would have.**

### **EMA Comment**

The EMA does not fundamentally object to the methodology for selection provided in the Draft RTS, which builds on the methodology laid down in the RTS under Article 40(2) of AMLD6, and supports the objective of establishing consistent risk assessment methodologies across the EU.

However, several aspects require careful consideration. The criteria for determining which entities fall within scope of direct supervision should be more concrete and quantifiable. The current draft RTS creates significant uncertainty for regulated entities trying to understand their obligations.

We recommend establishing clear, objective parameters with detailed guidance on practical application, ensuring consistent interpretation across Member States, and specific thresholds and risk factors that determine the scope of supervision. The risk assessment methodology should ensure proper granularity, including within specific sectors. A one-size-fits-all approach may not adequately capture varying risk profiles within the same industry or across different business models. The methodology should allow for differentiation based on actual operational models, and consider demonstrated risk levels and transaction patterns. This would enable proportionate application of requirements based on risk while maintaining effective AML/CFT controls.

Regarding methodology alignment, we note that adjustments based on the SNRA should be consistently permitted across different RTS. National specificities should be considered where appropriate, and group-wide risk assessment approaches should be harmonized between AMLA and national competent authorities. This alignment is crucial for ensuring effective and consistent application of AML/CFT controls across the EU. We believe these standards present an important opportunity to enhance the EU's AML/CFT framework. However, their effectiveness depends on maintaining a risk-based approach that enables obliged entities to allocate resources efficiently while ensuring robust controls where risks are highest. We urge careful consideration of the practical implementation challenges highlighted above to ensure the standards achieve their intended objectives without creating disproportionate operational burdens.

We would welcome further clarification within the RTS on how AMLA intends to collect the data required for its risk assessments under this framework. The RTS does not state whether the use of the same methodology implies reliance on the same data submissions already provided to national competent authorities, or whether obliged entities will be expected to report directly to AMLA in a separate or parallel process.

The RTS also does not clarify how or whether the risk assessment will align with obliged entities' own risk assessments under Article 10(4) AMLD6, or how disagreements between supervisors will be resolved. More guidance is needed early on to ensure coherence and help entities plan, especially those operating cross-border.

## Question 5

**Do you agree that the selection methodology should not allow the adjustment of the inherent risk score provided in Article 2 of draft under article 40(2) AMLD6? If you do not agree, please provide the rationale and evidence of the impact the EBA's proposal would have.**

### EMA Comment

The EMA does not support the prohibition of adjustments to inherent risk scores. In cases where quantitative data does not adequately capture a firm's true risk profile, qualitative overrides play a critical role. Any such overrides should be restricted to clearly defined circumstances, accompanied by well-documented justifications, and subject to approval at a senior level to ensure potential misuse.

## Question 6

**Do you agree with the methodology for the calculation of the group-wide score that is laid down in article 5 of the RTS? If you do not agree, please provide the rationale for it and provide evidence of the impact the EBA's proposal and your proposal would have.**

### EMA Comment

The EMA has concerns about the specific application of the three proposed metrics outlined in Article 5(3) such as: (i) total number of customers, (ii) total value of incoming and outgoing transactions, and (iii) total assets held or managed, as they may yield conflicting results and fail to accurately capture the individual risk contribution of each affiliate.

To improve the effectiveness of the methodology, we recommend adopting a more flexible framework that considers the most relevant and proportionate weighting factors per affiliate, taking into account the diversity of business models and risk profiles across a group.

## Question 7

**Do you have any concern with the identification of the group-wide perimeter? Please provide the rationale and the evidence to support your view on this.**

### EMA Comment

N/A

## Question 8

**Do you agree to give the same consideration to the parent company and the other entities of the group for the determination of the group-wide risk profile? Do you agree this would reliably assess the group-wide controls effectiveness even if the parent company has a low-relevant activity compared to the other entities?**

### EMA Comment

The EMA does not fundamentally object to the inclusion of the parent company in the determination of the group-wide risk profile. However, the parent company and its affiliates should not be given equal weight in group-wide risk assessments. Doing so may distort results as, for example, where non-EU entities provide different services or operate under divergent control environments. When assessing the residual risk of an EU-regulated entity, only its own control environment should be considered.

## Question 9

**Do you agree with the transitional rules set out in Article 6 of this RTS? In case you don't, please provide the rationale for it and provide evidence of the impact the EBA's proposal and your proposal would have.**

The EMA generally agrees with the transitional rules set out in Article 6 of the draft RTS. We also acknowledge the value of allowing adjustments to the controls' quality score based on the outcomes of on-site inspections conducted within the two years prior to the launch of assessments. This flexibility can help ensure that relevant supervisory insights are taken into account, especially where recent inspections reveal material control strengths.

However, we believe it is essential that entities are afforded the right to challenge any supervisory adjustments made under Article 6(2). The potential impact of a one-category adjustment, particularly where it leads to a reclassification of a firm's ML/TF risk profile, can be significant, influencing future supervisory intensity. A clear, fair mechanism for contesting such adjustments would support transparency and protect firms from disproportionate outcomes.

In addition, the interpretive notes to the RTS should include examples of the types of situations in which adjustments may be deemed appropriate. This would enhance clarity and consistency in the application of this provision, and help both firms and supervisors align expectations.

Provided that the transitional period is granted, we encourage the EBA to initiate a dry run exercise to identify an initial list of potentially affected entities. This would allow for practical testing of the transitional rules and enable any necessary adjustments prior to full implementation.

## **EMA Response to the Draft RTS on the assessment of the inherent and residual risk profile of obliged entities under **Article 40(2) of the AMLD****

### **Question 1**

Do you have any comments on the approach proposed by the EBA to assess and classify the risk profile of obliged entities?

#### **EMA Comment**

[TBC]

### **Question 2**

**Do you agree with the proposed relationship between inherent risk and residual risk, whereby residual risk can be lower, but never be higher, than inherent risk? Would you favour another approach instead, whereby the obliged entity's residual risk score can be worse than its inherent risk score? If so, please set out your rationale and provide evidence of the impact the EBA's proposal would have.**

#### **EMA Comment**

The EMA agrees with the proposed approach.

### **Question 3**

**Do you have any comments on the proposed list of data points in Annex I to this Consultation Paper? Specifically,**

- **What will be the impact, in terms of cost, for credit and financial institutions to provide this new set of data in the short, medium and long term?**

Short term, initial costs will primarily involve a gap analysis and investigation by each firm, and then where necessary changes to IT systems and (IT) development to support reporting capabilities. The upfront cost can be significant, but once the initial set of data has been generated, subsequent repetitions are likely to incur lower cost. Therefore, maintaining static data requirements is crucial to control ongoing costs, as any changes will necessitate further investment.

Smaller financial institutions will be disproportionately affected as they will not have the data requested readily available and are likely to have less resource at their disposal.

- **Among the data points listed in the Annex I to this consultation paper, what are those that are not currently available to most credit and financial institutions?**

In the absence of a more granular definition, it is challenging to make meaningful comments on the specific data points in the Annex I. The data will be supplemented by an interpretive note to further expand on the definition of the data requested: We understand that the draft interpretive note is currently being tested as part of a trial with a number of firms in Member states: Given that the data lacks definitions at present, the EMA believes that the industry should be given an opportunity to comment on the interpretive note and that the draft should be published. Transparent and consistent processes would result in clear and widely understood definitions that will improve the quality of the data submitted by the industry.

Smaller firms are less likely to have the data requested readily available and will therefore be affected disproportionately as they will have less resource available.

**Products, Services and Transactions** The data points on ‘Products, Services and Transactions’ could result in duplicate reporting: i.e. an e-money account that is also a payment account with a vIBAN and a prepaid card associated with it: transactions using such an account could be reported multiple times, inflating the size of individual firms and the industry as a whole. This is not an uncommon scenario. Another example is the number of customers using services for the exchange of fiat-crypto, crypto-fiat and crypto-crypto: One customer using all of these services would be reported three times, thus making the CASP’s customer base appear significantly larger than it actually is. The EBA should be mindful to avoid duplicate reporting.

The section singles out certain products without providing a rationale for doing so: e.g. vIBAN and prepaid cards are included in the dataset, but not credit cards, with no explanation. The products selected for reporting seem to signal potential risk associated with these products and adding them to the list makes them appear higher risk per se without a rationale or justification. The EBA should provide a justification for the dataset.

The e-money product data set uses terms that are ambiguous and not defined in an e-money context: e-money is issued (purchased), spent and/or redeemed (see Articles 2 and 11 2EMD DIRECTIVE 2009/110/EC). The EMA suggests that the EBA introduce terms that are defined in the Directive to avoid ambiguity.

*‘Total Number of e-money transactions by non-identified customers in the previous year; Value (EUR) of e-money transactions by non-identified customers in the previous year’* We would like to note that all e-money account holders are identified, although they may not all be verified for low risk products. We suggest that the EBA adjust the text accordingly.

*‘Total number of customers using prepaid cards with more than 3 prepaid cards’* whilst this could be an indicator of higher risk, such programmes could also be low- risk corporate expense

programmes. In the absence of a free text field or any way to explain the data reported, obliged entities could be assigned an inaccurate risk classification. Obligated entities should be awarded a mechanism to provide an interpretation of the data submitted e.g. in an accompanying letter or a free text field.

The AML/CTF Control data seems to mandate a standard approach to customer risk assessment when it asks for '*Number of customers per ML/TF risk category (low risk, medium-low risk, medium-high risk, high-risk)*'. Please note that obliged entities have different risk assessment methodologies and jurisdictions have different approaches towards categorisation e.g. Ireland have decided to apply L/M/H this could result in duplication of efforts.

- **To what extent could the data points listed in Annex I to this Consultation Paper be provided by the non-financial sector?**

Please provide evidence where possible.

#### **EMA Comment**

Not applicable.

### **Question 4**

**Do you have any comments on the proposed frequency at which risk profiles would be reviewed (once per year for the normal frequency and once every three years for the reduced frequency)? What would be the difference in the cost of compliance between the normal and reduced frequency? Please provide evidence.**

#### **EMA Comment**

The EMA welcomes the option for some smaller, low risk entities to submit data every three years as this will reduce cost and effort such as the resource needed to compile the report.

### **Question 5**

**Do you agree with the proposed criteria for the application of the reduced frequency? What alternative criteria would you propose? Please provide evidence.**

#### **EMA Comment**

The EMA agrees with the proposed criteria.

## Question 6

**When assessing the geographical risks to which obliged entities are exposed, should cross-border transactions linked with EEA jurisdictions be assessed differently than transactions linked with third countries? Please set out your rationale and provide evidence.**

### EMA Comment

The EMA's view is that cross-border transactions within the EEA - and with jurisdictions that are considered to have an AML/ CTF regime equivalent to that of the EU/ EEA Members States - warrant a different risk assessment than those involving third countries. The reasoning behind this approach is multifaceted:

**Consistent Regulation within the EEA:** EEA nations operate under a uniform AML/CFT framework, established by EU Money Laundering Directives and Regulation (EU) 2024/1624. This harmonization ensures equivalent rules and supervision across Member States, reducing regulatory ambiguities for financial entities. The establishment of AMLA further strengthens this by enhancing oversight of high-risk cross-border financial institutions and fostering collaboration among national authorities and Financial Intelligence Units (FIUs), thereby mitigating overall risk.

**Accurate Risk Profiling:** Applying uniform scrutiny to both EEA and third-country transactions distorts genuine risk profiles. Transactions within the EEA inherently benefit from shared legislative and supervisory mechanisms, leading to lower inherent geographical risk. A blanket approach would impose unnecessary operational burdens and result in disproportionate risk assessments, particularly impacting smaller cross-border institutions.

**Nuanced View of Third Countries:** The EMA emphasises that not all non-EEA jurisdictions should be automatically deemed high-risk. Some third countries possess AML/CTF regimes equivalent to those of EU/EEA Member States. Third countries should be evaluated individually using a clear, published methodology to assign appropriate risk ratings.

**Effective Resource Allocation:** Misdirecting resources towards low-risk EEA transactions can distract from essential efforts in genuinely higher-risk jurisdictions outside the EU/EEA, ultimately weakening an institution's overall risk management strategy.

It is essential to distinguish between EEA transactions and those involving third countries, with the understanding that third countries should not automatically be classified as high-risk. For intra-EEA relationships, a heightened risk classification should only occur based on evidence of jurisdiction-specific deficiencies or systemic threats that extend beyond their simple cross-border nature.

## **EMA response to Draft RTS under Article 28(1) of the AMLR on Customer Due Diligence**

Members of the EMA have expressed a common view on the erosion of the risk-based-approach (“RBA”) in both the AMLR and in the RTS. There is an increasing trend to specify data -such as place and country of birth, or documents -government issued ID, to erode the concept of SDD through specific examples, or the means of verification -through video sessions. This rule based approach can have the effect of discouraging firms from taking responsibility for the choices that they make, in favour of meeting specific obligations. We encourage more principles based provisions that requires firms to understand and effectively manage risk, while allowing them the flexibility to take specific actions and to allocate resources where they are most needed

### **Question I**

**Do you agree with the proposals as set out in Section I of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?**

#### **EMA Comment**

##### **I. Interpretative language**

Section I addresses the collection of information for the purpose of identification as well as the means of verification of such information by regulated entities. It is important to note that whilst the implementation of identification and verification obligations under Directive (EU) 2015/849 (“4MLD”) was both risk based and subject only to regulatory guidance, the present AMLR has taken a more restrictive approach to risk-based compliance and the present RTS, once adopted will have the status of a Regulation with direct effect.

Provisions in relation to implementation of CDD requirements – eg what are elements of identity, or what are the means of verification of identity information, become legislatively obligatory and restrict alternative means of implementation. Furthermore, any legal interpretations of the AMLR as legislative text become legislative obligations in themselves, and in one case –(see below) have led to a significant narrowing of legislative freedom, and a departure from the obligations under the FATF Forty. If this amounts to a departure from the risk based approach, it may be worth considering whether this also presents a risk for MSs undergoing mutual evaluation.

##### **Means of verification under the risk based approach**

The AMLRs provide at Article 22 for both the elements of ID that make up identification of natural and legal customers, **and also** at paragraph 6 for the means of undertaking verification.

*6. Obligated entities shall obtain the information, documents and data necessary for the verification of the identity of the customer and of any person purporting to act on their behalf through either of the following means:*

*(a) the submission of an identity document, passport or equivalent and, where relevant, the acquisition of information from reliable and independent sources, whether accessed directly or provided by the customer;*

*(b) the use of electronic identification means which meet the requirements of Regulation (EU) No 910/2014 with regard to the assurance levels ‘substantial’ or ‘high’ and relevant qualified trust services as set out in that Regulation.*

Paragraph 22(6)(b) provides for the use of eIDAS Regulation, which has now been amended by Regulation (EU) 2024/1183 of 11 April 2024 establishing the European Digital Identity Framework. This is required to be implemented by way of digital identity wallet issuance by 28 October 2026.

We anticipate that use of digital ID wallets for onboarding by EU customers will take some time to become commonplace, and even if digital ID wallets are available by the beginning of 2027, it is likely that use of existing means of ID are likely to continue in parallel for some time.

There is therefore dependence on the provisions of Article 22(6)(a) for:

- (i) Those customers that do not yet have access to a digital ID Wallet
- (ii) Customers who do not wish to use a digital ID Wallet
- (iii) Existing records of customers who have been verified using existing means –(all current customers), and for whom obliged entities must meet the new standards under the AMLR within 5 years as set out under Article 22(2) of the draft RTS.

Article 22(6)(a) provides for verification using “...an identity document, passport or equivalent and, where relevant, the acquisition of information from reliable and independent sources...”

**Issue: Article 5 of the RTS adopts an interpretation of Article 22(6)(a) above that suggests that ‘...and, where relevant...’ indicates an additive clause.** In other words that verification must always be by way of an identity document, and where relevant, additional means of verification can be applied using information from reliable independent sources.

- (a) A review of the text suggests this is only one possible interpretation of the clause, and that this interpretation overly restricts the means of verification that can be applied by obliged entities.

To this extent, there is an equally valid reading of the same words that suggests that reliable and independent sources of information are a valid **alternative** to government issued ID. It does not need to be the case that independent reliable information can only be of value AFTER government ID has been obtained.

This meaning can be demonstrated by adopting the same sentence structure in other contexts, for example, one can say:

- In the summer it is usual to wear shorts and, where relevant, to wear trousers
- It is healthy to walk to work and, where relevant, to cycle
- High school students often go to university and, where relevant, to technical colleges

We do not suggest that the sole intention was to make the ‘and’ mean the alternative, but rather that it can carry both an ‘additive’ and ‘alternative’ meaning, and the RTS which once a Regulation will have direct legal effect, should not restrict the options available to obliged entities. It should allow for both interpretations to co-exist under Article 22(6)(a)).

- (b) Current legislation, 4MLD clearly provides that the means of verification should be from data or information obtained from a reliable and independent source. Article 13(1)(a) 4MLD.
- (c) Recommendation 10 of the FATF Forty, provides that verification of identity should be undertaken “using reliable, independent source documents or information”.
- (d) FATF Recommendation 1, in turn, provides that the RBA should be an essential foundation to the efficient allocation of resources across the AMML/CTF regime”. It also provides in the same paragraph that “where countries identify lower risks, they should allow and encourage simplified measure as appropriate”.

It follows therefore that restricting verification of ID to always requiring government issued ID or similar is overly restrictive, and risks being inconsistent with the RBA.

- (e) The issue becomes more pronounced when this requirement is applied in a non-face-to-face environment. This is the wide-spread means of engagement between obliged entities and their customers, and because of the insistence on using government issued ID, the only means of verification that is provided for in the RTS under Article 22(6)(a) is that of creating a video session with the customer, with various assurances being required to ensure authenticity.

This method has often been costly, slow, and unwieldy. Furthermore, where the risk is low, say the purchase of some insurance or limited functionality payment products, the cost of each instance will be significant. The ability to utilise a broader choice of verification methods is required to benefit from the RBA.

Furthermore, the risk of Deep Fakes is increasingly significant. A recent consumer report - (‘Trust in the Digital Economy’ <https://www.checkout.com/guides-and-reports/digital-economy-report>), commissioned by Checkout.com in collaboration with YouGov suggested that over 50% of UK adults are concerned over Deep Fake scams, and similarly over theft of their likeness. It would not be prudent to rely entirely on any one method of ID verification, and not on one that is becoming more vulnerable to attack over time, or that may not have consumer trust. It would be preferable to provide for diverse means of verification that allowed for varied and

robust processes to be developed by industry and which could combat threats as they arose.

We suggest avoidance of mandating one or more means at such a detailed level, and allowing industry to evolve techniques and approaches to verification that can stay ahead of fraudsters' threats over time. There is a risk that mandating any single approach will have the inadvertent effect of compromising industry's defences and disincentivise

- (f) Given that verification of identity for legacy (existing) customers of obliged entities will need to comply with the new requirements within 5 years, it will make a big difference for firms whether non-government ID records are going to be acceptable under the new regime. The number of records that will have to be renewed could be significantly higher and the costs associated with bringing such records up to date will be a significant proportion of the compliance budget of many obliged entities.

This is again exacerbated for non-face to face customers, whose records may even include evidence based on government issued ID, but which were not verified in accordance with Article 6 of the RTS, using video sessions. The cost for this process is likely to be significant, and may not add much value, particularly where evidence of ID has already been reinforced by other factors established over the course of the relationship. A more risk-based approach would allow for better allocation of resources.

## Conclusion

**The approach to the interpretation of Article 22(6)(a) would benefit from review, with a view to adopting a more inclusive approach to verification of ID, one that allows for diverse processes to be developed, immediate reaction to evolving security threats and consistent with a broader interpretation of the legislative text. Implementation can better recognise the value of information collected over time, and allow for a risk-based approach in relation to legacy records.**

## Further comments

**Article 6(3)** provides for requiring explicit consent before remote verification is undertaken. Consent will already have been obtained through the terms of service, and the GDPR allows for such processes to be undertaken. We suggest removing this requirement.

## Question 2

**Do you have any comments regarding Article 6 on the verification of the customer in a non face-to-face context? Do you think that the remote solutions, as described under Article 6 paragraphs 2-6 would provide the same level of protection against identity fraud as the electronic identification means described under Article 6 paragraph 1 (i.e. e-IDAS compliant solutions)? Do you think that the use of such remote solutions should be considered only temporary, until such time when e-IDAS compliant solutions are made available? Please explain your reasoning.**

### EMA Comment

Please refer to our response to question 1 above, and in particular on restricting non face to face verification to essentially a single solution, in the absence of an eIDAS compliant, widely accepted approach.

Even when a digital ID based solution is available, there should be a diversity of options to minimise the likelihood of compromise and to increase resilience. Many verification products will collect data from diverse sources and combine it with geolocation and behavioural metrics to obtain a strong means of verification.

There will always be circumstances where eIDAS is not available, and video means of verification is only appropriate in a limited set of circumstances; as well as being undermined by AI and deepfake technology.

There are also limitations to eIDAS in terms of implementation and integration. The adoption of a framework across multiple member states, operated by multiple entities and consumed by a range of businesses will be challenging. It will be some time before it can become sufficiently dependable to act as a defacto means of verification. Similarly application to businesses and legal entities is yet to be addressed.

## Question 3

**Do you have any comments regarding Article 8 on virtual IBANS? If so, please explain your reasoning.**

### EMA Comment

Article 8 provisions allowing account holding payment service providers to make information available to vIBAN issuing institutions within the 5 working days specified in the AMLR is helpful. The text is however open to being interpreted by member states or vIBAN issuers as giving them the right to require firms using vIBANs to provide the information within a shorter time period than that allowed. Clarity in this regard would be helpful.

## Other issues in section I:

**Article 3:** requirement for the place of birth to consist of both the city and country of birth.

**Issue:** Many passports and other government issued ID do not provide for both data elements; we suggest that either city or country of birth be sufficient. In most cases only the city is provided.

**Article 4:** requirement to obtain the nationalities of customers has been expressed as requiring obliged entities to **satisfy themselves that they know of any other nationalities** that the customer holds. This level of certainty is not risk based, and meeting this level of certainty is almost impossible in the absence of nationality registers. We suggest reliance on information provided by the customer.

**Article 11:** The criteria for concluding that an ownership structure is complex includes that: “there are indications of non-transparent ownership with no legitimate economic rationale or justification”. We suggest that this criterion is broadened to allow for structures that may seek to protect the identity or security of individuals, provided these are justified. The threshold for performing such diligence is also only expressed in terms of complexity and not in terms of risk. It may be that the relationship does not pose any significant risk, nor is associated with significant payments. In such circumstances, the PSP should be in a position to apply a risk based decision, and choose not to enquire into the structure.

## Question 4

**Do you agree with the proposals as set out in Section 2 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?**

### EMA Comment

Article 15 deals with the purpose and intended nature of the customer relationship and flows from AMLR Article 21(c). Article 15(d) provides for an enquiry into the source of wealth, which appears to be unrelated to the specific objective. It may be appropriate in certain EDD circumstances where the origin of funds needs to be established, but is disproportionate when assessing the nature of the relationship.

## Question 5

**Do you agree with the proposals as set out in Section 3 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?**

## EMA Comment

We note the amendment of level 1 text to make the identification of PEPs non risk-based; this is contrary to the RBA but this issue is mostly not in scope of the RTS. One issue that does arise however and which is addressed below at Section 4 under provisions for SDD and set out at Article 20 for pooled accounts. The approach to pooled accounts is contrary to EU policy of seeking to address de-risking in the banking sector, and it will be made more onerous by PEP provisions that would apply as a result of the RTS's approach to pooled accounts.

## Question 6

**Do you agree with the proposals as set out in Section 4 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?**

## EMA Comment

The AMLR has moved away from a RBA by specifying the circumstances under which SDD could be exercised by firms. Instead of allowing flexibility and the ability to divert resources to where there is greater risk; this is now only possible where the specific examples of low risk are met:

These are set out at Article 33(1) summarised as:

- (a) Postponing verification to no longer than 60 days from establishing a business relationship
- (b) Reducing the frequency of customer identification updates
- (c) Inferring the purpose of a business relationship or reducing the information collected
- (d) Reducing scrutiny or frequency of monitoring transactions
- (e) Applying any other SDD measure identified by AMLA

The final example, allows AMLA/EBA to exercise judgement and to provide for a broader set of circumstances that could be useful for industry and ultimately create a more effective use of resources and a RBA.

Two areas that would benefit from SDD would be (i) the elements of ID that are required to be collected and (ii) the extent of verification of these elements. This would be helpful and effective in implementing the RBA across the varied products, business models, channels and jurisdictions.

This has been exercised to some extent under Article 18 of the RTS where the home address of a natural person does not need to be collected and, similarly for legal entities the shareholders and legal representatives are not required to be identified. This is supported as a proportionate means of reducing the burden of identification under SDD conditions.

It would however be helpful to give further flexibility in relation to the extent of verification that would be required under SDD provisions. There are many ways of verifying identity that do not involve obtaining government ID and which enable a reasonable degree of verification to be exercised, in a manner that is risk based.

The payments industry has for example utilised evidence of access to a bank account in the name of the customer as a limited degree of due diligence, given that the bank will have undertaken full CDD on the customer on account opening. Such approaches have been key in encouraging onboarding of customers where the risk is low, and often act as a means of entry, whereby further CDD is undertaken once the risk or activity is increased.

We encourage the EBA to assess the success of such approaches and to consider providing for continuity for current practices.

## Question 7

**What are the specific sectors or financial products or services which, because they are associated with lower ML/TF risks, should benefit from specific sectoral simplified due diligence measures to be explicitly spelled out under Section 4 of the draft RTS? Please explain your rationale and provide evidence.**

### EMA Comment

**General response:** previous legislation has provided for such a list which includes: life insurance policies, other specific insurance products, pensions under certain conditions on transferability, and products intended to address financial inclusion.

We concur with the above list.

We suggest additionally however that SDD be implemented in broader manner, providing for its application to products that can demonstrate effective risk identification and mitigation so as to present a low ongoing risk of money laundering. This can be set out as a number of conditions that must be satisfied, which if met, allow for SDD to be adopted. It would allow a more flexible application on the one hand, and a more accountable outcome on the other. Obligated entities can be given more flexibility in applying SDD whilst being held to account for how it is applied.

### Pooled accounts:

Article 20 of the RTS contemplates the obligations of a credit institution (“CI”) that is operating a pooled account belonging to a third party, addressing the CI’s obligations under AMLR Article 20(1)(h) which provides:

*“(h) where a transaction or activity is being conducted on behalf of or for the benefit of natural persons other than the customer; identifying and verifying the identity of those natural persons;”*

The RTS begins with an assumption that this article should apply to CI that hold client funds belonging to other regulated payment service providers, and then proceeds to define conditions that could be applied to such a relationship that would result in the arrangement being considered low risk and meriting SDD.

### Issues that arise:

There are significant issues associated with the assumption that is made on the one hand, and then with the outcome of codifying this single interpretation into a Regulation that has direct effect.

- I. The application of AMLR Article 20(1)(h) to the relationship between a CI and a regulated payment service provider by way of a pooled account is problematic for two main reasons:
  - i. Transactions conducted by the CI on behalf of the PSP can only be regarded as services for the PSP itself. The benefits that accrue to the clients of the PSP are services provided by the PSP itself not by the CI. The PSP is the party that is regulated to provide these services to its customers. The CI on the other hand provides services to the PSP, it does not conduct services “...on behalf of or for the benefit of natural persons other than the customer...”<sup>[1]</sup>
  - ii. Secondly, The PSP is regulated prudentially by its NCA for the provision of payment services, it is also regulated for conduct of business risk, being subject to consumer related obligations, ensuring that the payment is executed in accordance to legislative expectations and users have expectations to service levels as well as dispute resolution mechanisms. Furthermore, the PSP is regulated under financial crime legislation including the AMLR, and is obligated to undertake CDD, to perform transaction monitoring, make suspicious activity reports, keep records etc.

Interpreting Article AMLR 20(1)(h) so as to introduce a CDD obligation on the CI in relation to the customers of the regulated PSP is inappropriate, disproportionate and calls into question the purpose of the regulatory regime to which the PSP is subject. Exactly the same regime to which the CI is subject.

This provision calls into question the role of the NCA and the authorisation regime to which the PSP is subject. If either the legislative provisions are inadequate or the NCA is not enforcing well enough, then these shortcomings should be addressed. It is not the place of one sector to police another.

2. It then follows that seeking to define conditions under which a CI can regard itself as fulfilling such expectations, reinforces this disproportionate interpretation and creates a

---

<sup>1</sup> AMLR Article 20(1)(h)

significant barrier to service delivery. CIs under this interpretation have no incentive to offer banking services to PSPs, and if they do, to do so by levying significant fees on the PSP service, that reflects the AML/CTF compliance risk that they will be subject to. This of course then propagates to the price of the service offering to consumers.

3. The conditions that are proposed to CIs at Article 20 of the RTS as a means of meeting compliance obligations, act to calibrate CI's expectations in relation to the extent of PSP compliance risk they might reasonably take-on and the type of controls they might be expected to put in place to mitigate this compliance risk.

Article 20 provides that CIs can regard compliance obligations as having been met provided:

- i. The customer (PSP) will provide them with CDD information on its own customers immediately upon request
- ii. The customer (PSP) is an obliged subject to AML/CFT obligations in the EU or an equivalent regime
- iii. The customer is effectively supervised for compliance
- iv. The ML/TF risk associated with the business relationship is low
- v. The CI is satisfied that its customer applies robust and risk sensitive CDD on its own customers and UBOs.

It follows therefore that a CI contemplating offering banking services to an EU PSP will likely only do so to PSPs that operate in a low-risk environment as per (iv), that it examines the compliance policies of the PSP, assesses its implementation of its policies in order to meet requirements under paragraph (iii). Furthermore, it must conduct periodic audits of the PSP's compliance with CDD obligations in order to confirm the requirements of paragraph (v) are met.

Finally any such customer PSP must also be subject to the same oversight in the EU as the CI, or a jurisdiction applying equivalent or more robust regulation.

What part of the AML regulatory regime requires that firms that are equally subject to it, are placed in a hierarchical order of perceived effective compliance? This distorts the playing field and is not consistent with a number of principles of EU law.

## Conclusion

It is our view that interpreting Article AMLR 20(1)(h) so as to introduce compliance obligations for CI over other PSPs has little basis in EU legislation. It may suggest that NCAs are unable to fulfil their role in supervising PSPs, and this must therefore be 'outsourced' to CIs. This Article is better struck out in its entirety. Keeping it is likely to reduce competition in the payments space, increase the incidence of de-risking in the banking environment and increase the cost of payments to

end-users. It would also distort the playing field and be inconsistent with provisions on banking access set out in PSD2 and PSR/PSD3.

### **Compliance for existing customers**

Article 22(2) provides for a five year period within which all existing customer records have to be brought up to date with new requirements. This relates to both the extent of identification information that is collected, and the more restrictive means by which verification can be implemented.

This will likely be a significant endeavour, and one which would benefit from a risk based approach; where:

- i. Customer records for those that present medium and high levels of risk are updated when there is some interaction with them, whether through customer service, new products or other initiatives
- ii. Low risk customers present a low risk of ML/CTF and may not need to be updated unless contracts are renewed or new products are offered
- iii. The period for compliance is increased to 10 years to allow for a natural migration to the new requirements.

### **Question 8**

**Do you agree with the proposals as set out in Section 5 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?**

#### **EMA Comment**

We do not have any substantive comments on this section.

Article 24(d) requires, in the event of financial crime being suspected for specific information to be obtained about the customer that may only be available from the customer themselves. This could of course inadvertently lead to tipping off and further development of this provision would be helpful.

### **Question 9**

**Do you agree with the proposals as set out in Section 6 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?**

## EMA Comment

Comments on this section will follow.

## Question 10

**Do you agree with the proposals as set out in Section 7 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?**

## EMA Comment

The exemption for low value electronic money instruments is based on a number of restrictions that are referred to as “risk mitigating measures” in AMLR Article 19(7). The Article states:

*“7. Supervisors may, directly or in cooperation with other authorities in that Member State, exempt obliged entities from applying, in full or in part, the customer due diligence measures referred to in Article 20(1), points (a), (b) and (c), with respect to electronic money on the basis of the proven low risk posed by the nature of the product, where all of the following risk-mitigating conditions are met:”*

The conditions are as follows:

- The amount stored does not exceed EUR 150
- The instrument is used exclusively to purchase goods and services
- The instrument is not linked to another payment account and cannot be used to exchange for cash or to purchase crypto assets
- The products is subject to transaction monitoring

The mandate at Article 28(1)(c) of the AMLR states:

*“ Those draft regulatory technical standards shall specify:*

*(c) the risk factors associated with features of electronic money instruments that should be taken into account by supervisors when determining the extent of the exemption under Article 19(7);”*

Level I text has set very limited parameters under which exemption can be granted, we are not of the opinion that the intention of the AMLR text is for further factors to be added. Rather, it is to ensure that the implementation of the exclusion does not undermine its objectives.

In relation to the factors set out at Article 30:

- a. This should be removed as the AMLR already provides for a low limit of EUR 150

- b. Whilst funding from an own account evidences reduced risk, most funding of such instruments will be at POS terminals and it would not be possible to asset; these products also enable financial inclusion and this should not be undermined through such a factor. We suggest this factor is removed.
- The charge made for product has no impact on its risk, this should be removed.
- The limited network exemption renders products excluded from the scope of payments regulation, and there would be no AML.CTF regulation in any event. This should be removed.
- Products should be used to support the single market and issuers should not be precluded from supporting such use; we suggest this is removed
- All such products have a limited duration, this does not however impact AML/CTF risk meaningfully, and is better removed.
- Distributors are not regulated and suggesting such a feature will be of little assistance. This should be removed
- Restriction of purchases outside the Union does not limit risk; perhaps restricting to high risk jurisdictions may have an impact; but purchases in Switzerland or the UK for example should not be discriminated against.

Risk factors can for example seek to ensure that:

- Controls are in place to restrict use to the purchase of goods and services
- Whilst the total storage limit does contemplate multiple instruments being purchased, these should not be so as to abuse the limits set
- Transaction monitoring of both purchase and redemption transactions
- Acceptance should be further scrutinised where it represents a higher risk activity

## Question 11

**Do you agree with the proposals as set out in Section 8 of the draft RTS (and in Annex I linked to it)? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?**

### EMA response

We do not have any comments on this section at this time.

## Members of the EMA, as of June 2025

Airbnb Inc	MONETLEY LTD
Aircash	Moneyhub Financial Technology Ltd
Airwallex (UK) Limited	Moorwand Ltd
Amazon	MuchBetter
Ambr	myPOS Payments Ltd
American Express	Navro Group Limited
Banked	Nuvei Financial Services Ltd
Benjamin Finance Ltd.	OFX
Bitstamp	OKG Payment Services Ltd
Blackhawk Network EMEA Limited	OpenPayd
Boku Inc	Owl Payments Europe Limited
Booking Holdings Financial Services International Limited	Own.Solutions
BVNK	Papaya Global / Azimo
Cardaq Ltd	Park Card Services Limited
CashFlows	Payhawk Financial Services Limited
Circle	Paymentsense Limited
Coinbase	Payoneer Europe Limited
Crypto.com	PayPal
Currenxie Technologies Limited	Paysafe Group
Curve UK LTD	Paysend EU DAC
Decta Limited	Plaid B.V.
Deel	Pleo Financial Services A/S
eBay Sarl	PPS
ECOMMPAY Limited	Push Labs Limited
emerchantpay Group Ltd	Remitly
EPG Financial Services Limited	Revolut
eToro Money	Ripple
Etsy Ireland UC	Satispay Europe S.A.
Euronet Worldwide Inc	Securiclick Limited
Finance Incorporated Limited	Segpay
Financial House Limited	Soldo Financial Services Ireland DAC
FinXP	Square
First Rate Exchange Services	Stripe
Fiserv	SumUp Limited
Flywire	Syspay Ltd
Gemini	TransactPay
Globepay Limited	TransferGo Ltd
GoCardless Ltd	TransferMate Global Payments
Google Payment Ltd	TrueLayer Limited
IDT Financial Services Limited	Uber BV
iFAST Global Bank Limited	Unzer Luxembourg SA
Imagor SA	VallettaPay
Ixaris Systems Ltd	Vitesse PSP Ltd
J. P. Morgan Mobility Payments Solutions S. A.	Viva Payments SA
Kraken	Weavr Limited
Lightspark Group, Inc.	WEX Europe UK Limited
Modulr Finance B.V.	Wise
MONAVATE	WorldFirst
	Worldpay