Contribution ID: 80b53636-2838-41bd-8c07-c3d4f546b548
Date: 08/05/2026 20:51:24

Public Consultation on the draft Regulatory Technical Standards on Customer Due Diligence under Article 28(1) of Regulation (EU) 2024/1624

Fields marked with * are mandatory.

Public Consultation on the draft RTS on Customer Due Diligence under Article 28(1) AMLR

Objective of the consultation

AMLA would like to receive feedback on provisions of the draft RTS under Article 28(1) of Regulation (EU) 2024/1624 ('AMLR') and in particular on the specific questions set out below.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices AMLA should consider.

Such comments should be sent by **8 May 2026, 23:59 (CET).**

Personal data protection:

The protection of individuals with regard to the processing of personal data by the AMLA is based on Regulation (EU) 2018/1725. Further information on the processing of the personal data is available in the Data Protection Notice.

All legal details can be found in our Specific Privacy Statement (SPS).

How to provide feedback

All the fields marked with an asterisk (*) are mandatory. If a question is not relevant for you, please answer with "NA".

We are using a survey format to help us analyse feedback effectively and efficiently. For this reason, document uploads are not enabled for this exercise, and we kindly invite you to share your comments directly within the survey.

Please note that by submitting your contribution, you acknowledge that it will be published on AMLA's website. Contributions will always be published. The name of organisations submitting their contribution will also always be published. The name of the natural person providing a contribution will be published unless they object to said publication. Please refrain from inserting further personal information beyond what we ask from you. In particular, please refrain from providing confidential information or special categories of personal data (that is "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"). Your email address will never be published.

Before publication, AMLA staff will perform a limited screening of all contributions provided for the sole purpose of filtering any inappropriate submissions. After this, the replies are made available to the public directly on AMLA's public consultations page.

Please note that your contribution may be subject to a request for access to documents under Regulation 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

Language disclaimer

AMLA welcomes submissions in all official EU languages. You can change the displayed language of this public consultation using the language selector in the top right corner of the EU Survey platform. Please note that all language versions other than English have been produced using machine translation and may contain inaccuracies. When in doubt, please refer to the English version.

Should you encounter issues with submitting your responses, please contact us by email at public.consultations@amla.europa.eu no later than 48 hours before the deadline of the consultation period.

Section 1 - Respondent profile

* This contribution is made by:

An organisation

* Name of the organisation

200 character(s) maximum

Electronic Money Association

* First name of individual (individual respondent or representative of organisation)

100 character(s) maximum

Judith

* Surname of individual (individual respondent or representative of organisation)

100 character(s) maximum

Crawford

* Email (note that your email address will not be published)

100 character(s) maximum

judith.crawford@e-ma.org

* Publication of your name and surname

- (●) I agree to the publication of my name and surname (note that your email address will never be published).
- ( ) Contribution to be published without my name and surname (note that your email address will never be published).

* Which of the following best describes your activity or organisation? Obliged entities are those listed in Article 3 of Regulation (EU) 2024/1624.

Maximum 1 selection(s)

- [ ] Obliged entity in the non-financial sector
- [ ] Obliged entity in the financial sector
- [ ] Self-regulatory body in the sense of Regulation (EU) 2024/1624 Article 2(1) point (47)
- [ ] Industry association representing non-financial sector obliged entities
- [x] Industry association representing financial sector obliged entities
- [ ] Civil society organisation/non-governmental organisation
- [ ] Other

* Financial sector

Maximum 11 selection(s)

- [ ] Credit institution
- [x] Consumer credit, factoring, payment services, guarantees, money market instrument, foreign exchange, electronic money
- [ ] Insurance
- [ ] Insurance intermediaries
- [ ] Investment firms

- [ ] Collective investment
- [ ] Central securities depositories
- [ ] Creditors
- [ ] Credit intermediaries
- [x] Crypto assets service providers
- [ ] Cross-border branches of financial institutions

* Please select the country from which you or your organisation carry out your main activities:

BE - Belgium

Section 2 - Substantive comments on the draft Regulatory Technical Standards

* 1. Do you agree that the proposals set out in these draft RTS can be applied across the range of products and services provided by your obliged entity?
If you do not agree, please:
(i) explain why the current proposals do not provide sufficient flexibility; and
(ii) provide concrete drafting proposals and explain why the specific measures you propose would be more appropriate.

Provisions that are clearly marked as applying only to a specific sector or service should not be taken into consideration if they do not impact your sector.

5000 character(s) maximum

Some of the proposals set out in the RTS are too limiting or prescriptive to be practicable. We have set out our comments and proposed amendments in more detail against each relevant RTS Article under "additional input". Please see our comments on Articles 2, 6, 11, 12, 30

In particular we consider that the obligation to use eIDAS-compliant digital ID for remote onboarding is not possible in many (if not most) EU member states and/or EU customers. Our comments are set out in more detail under our comments on Article 7.

* 2. Do you agree that the proposals set out in these draft RTS allow for the effective application of a risk-based approach towards compliance with AML/CFT requirements?
If you do not agree, please:
(i) specify the provisions concerned; and
(ii) provide concrete drafting proposals and explain why the specific measures you propose would be more appropriate.

5000 character(s) maximum

Some of the proposals set out in the RTS are too prescriptive so as to remove firms' ability to apply a risk-based approach.

In particular, some of the factors listed in Article 31 on the e-money exemption from CDD are so specific as to remove any possibility to apply a risk-based approach.

We have set out our comments and proposed amendments in more detail against each relevant RTS Article under "additional input". Please see our comments on Article 5, 9, 18, 31.

* 3. Considering the nature of your business, including its size, risks, and complexity, are there any situations where the information to be collected for the purposes of customer due diligence as proposed in these draft RTS is routinely unavailable and the proposals in these draft RTS do not provide an alternative solution? If so, please provide concrete examples of such situations and your proposals for alternative solutions.

5000 character(s) maximum

We continue to be concerned by the absence of any meaningful alternative to electronic identification means that meet the requirements of Regulation (EU) No 910/2014 (Art. 22(6)(b) AMLRs) where these are either unavailable or cannot reasonably be expected to be provided. In the light of the anticipated difficulties in cross-border use of the EU Digital Identity Wallet, whether within or outside of the EU, availability of such an alternative becomes an ever more pressing issue. In this respect, the alternative provided in Arts 7(2)-(4) RTS is too restrictive in that it mandates reliance on an official identity document. This precludes use of other available digital means of verification that may be less costly and more appropriate to the nature and risks of products offered (particularly where there is a low risk of identity theft). To use such alternative means is consistent with a risk-based approach, which suggests focusing resources on areas where they are most likely to prevent financial crime, as well as with the principle of technological neutrality, which has guided EU policy on remote onboarding to date.

In this context, it is important to note that it is now possible for information provided by a customer to be augmented with information available from reliable third-party sources and other signals that can be collected in real time during the onboarding process (including geographic indicators, online presence, etc.) These inputs can be ingested and validated holistically in a manner that allows for a better understanding to be obtained of a customer's identity and profile (and therefore potential financial crime risk) at a lower cost (which may be appropriate in the context of certain products), while also improving the experience for the customer. Overdependence on the submission of identity documents risks reducing the scope for further innovation in new identity verification measures and processes – to date, a notable strength of EU firms in comparison to peers in other regions – at a time when greater innovation and development in this space is possible now more than ever before.

As we have raised in our previous submissions, this issue is of great importance to FinTech firms because it: (i) impacts firms' ability to onboard new customers and thus their ability to scale their businesses, (ii) restricts their ability to employ innovative means of verification, (iii) impacts the costs of carrying out CDD, and (iv) disrupts the consumer journey, discouraging the taking up a payment product. One of our larger members estimates that they will incur an ongoing additional cost of 2.3M EUR per year given the manual review process that is required in instances when the user is not able to utilize an identification document that complies with a high level of assurance.

We therefore urge you to reconsider your approach to mandatory use of an official identity document. The RTS should explicitly recognise that in some circumstances a combination of customer-declared and implicit, programmatically collected data is a valid and proportionate basis for CDD, and that formal document verification is not required as a universal step in all cases.

Our members currently employ the following alternative means of verification. The RTS should allow flexibility for their use without prescribing any one means:

- Reliance on the funding account by establishing that a funding bank account with an EEA credit institution is in the name/control of the account holder;
- Database verification based on reliable credit and government sources;
- Cross-checks between digital footprint data (such as IP address, biometrics) and other elements of ID and of documentation, such as where the residential address is not stated on the official ID document; and
- AI/ML-based assurances.

* 4. Considering AMLA's legal mandate in Article 28(1) of Regulation (EU) 2024/1624, and taking into account your obliged entities' products offered and service provided, what other simplified due diligence measures should be included in the draft RTS, for example because of the associated lower ML/TF risks of these

products and services? Please provide concrete drafting proposals and rationale for the specific measures you would propose.

5000 character(s) maximum

Limited use of a payment product warrants the application of SDD until a customer has reached a threshold of use that could potentially bring it within one of the known ML/TF typologies. Before that point, there is not only little risk of financial crime, but the cost of conducting CDD (both monetary and in term of customer experience) far exceeds the value thereby added. We therefore suggest that AMLA utilise its mandate under

Art. 28(1)(b) AMLRs to identify additional SDD measures for small merchants (such as digital platform developers) or private sellers who receive payments in exchange for goods or services, up to a cumulative annual transaction threshold of EUR 1,000, as long as no money can be withdrawn from their account before full CDD is completed.

* 5. Additional observations: Do you have any additional comments relevant to the draft RTS that have not been covered above? Please ensure that comments refer to a specific article, are precise, and, where possible, supported by evidence. Where necessary, comments should also include a proposed solution.

5000 character(s) maximum

All of our detailed comments are set out beside the relevant Articles under "additional input"

Section 3 - Additional substantive input

Use this section to provide feedback on specific articles of the draft RTS, in case these were not already covered in your responses to the previous questions.

For each reply, please describe the issue identified, indicating, where relevant, whether it relates to legal certainty, proportionality, technical implementation or other factors. You are kindly asked to provide alternative drafting proposals and to explain why your proposal would be more appropriate.

Do you have any comments on a specific article in the draft RTS? There is no need to repeat comments made in the previous sections of this survey.

- (●) Yes
- ( ) No

* Please state the article number in simple figures, without referring to the subparagraphs or points (e.g. '3' or '21')

Only values between 1 and 33 are allowed

2

* Please share your comments below, specifying the subparagraph and point, if applicable (e.g. paragraph 1 point (a)).

5000 character(s) maximum

Article 2 RTS – Definition of persons acting on behalf of

We propose an amendment to Art. 2 RTS to clarify that the requirement in Arts 20(1)(i) and 22(1) AMLRs to verify 'that any person purporting to act on behalf of the customer is so authorised and identify and verify their identity' does not apply to legal representatives (e.g., Directors) and other authorised signatories (e.g., employees or staff empowered to request the issuance of corporate expense cards from a payment service provider) of the customer. This is in order to avoid unnecessarily extending CDD requirements to a potentially large group of corporate customer employees or staff. Such a clarification accords with the text of Recital 12 RTS and is also currently being made in relation to the equivalent UK provisions, which are based on the EU's AML regime.

Furthermore, we propose an amendment to Art. 2 RTS to clarify that the legal representatives whose names must be obtained under Art. 22(1)(b)(iii) AMLRs are only those relevant to the business relationship in question. Multinational corporations and other large corporate clients often have extensive lists of statutory legal representatives, many of whom have no connection to, or oversight of, the specific business relationship being established with the obliged entity.

Suggested alternative drafting (new text in CAPITALS):

Article 2 - Information to be obtained in relation to names

1. OBLIGED ENTITIES SHALL NOT REGARD NATURAL PERSONS THAT ARE LEGAL REPRESENTATIVES OR OTHERWISE TO ACT ON BEHALF OF CUSTOMERS THAT ARE LEGAL PERSONS AS FALLING WITHIN THE CATEGORY OF 'ANY PERSON PURPORTING TO ACT ON BEHALF OF INDIVIDUALS (FOR EXAMPLE WHEN THE INDIVIDUAL HAS GRANTED A POWER OF ATTORNEY TO ANOTHER INDIVIDUAL OR ENTITY) OR TO THIRD PARTIES ACTING ON BEHALF OF AN ENTITY (FOR EXAMPLE WHEN AN AGENT OR INTERMEDIARY ACTS FOR A COMPANY). EMPLOYEES OR STAFF OF A LEGAL PERSON ACTING ON ITS OWN BEHALF SHOULD BE CONSIDERED TO BE ACTING AS THE ENTITY.

2. In relation to the names and surnames of a natural person as referred to in Article 22(1), point (a)(i), of Regulation (EU) 2024/1624, obliged entities shall obtain all names and surnames that feature on the identity document, passport or equivalent.

3. In relation to the name of a legal entity as referred to in Article 22(1), point (b)(i), and other organisations that have legal capacity under national law as referred to in Article 22(1), point (d)(i), of Regulation (EU) 2024/1624, obliged entities shall obtain the registered name and the trade name where it differs from the registered name.

4. IN RELATION TO THE NAME OF LEGAL REPRESENTATIVES AS REFERRED TO IN ARTICLE 22(1), POINT (B)(III), OBLIGED ENTITIES SHALL ONLY OBTAIN THE NAMES OF THOSE REPRESENTATIVES RELEVANT TO THE BUSINESS RELATIONSHIP IN QUESTION.

Do you have any other comments on a specific article in the draft RTS?

- (●) Yes
- ( ) No

* Please state the article number in simple figures, without referring to the subparagraphs or points (e.g. '3' or '21')

Only values between 1 and 33 are allowed

5

* Please share your comments below, specifying the subparagraph and point, if applicable (e.g. paragraph 1 point (a)).

5000 character(s) maximum

Article 5 RTS – Verification of nationalities

Art. 22(1)(a)(iii) AMLRs does not refer to 'all' nationalities but merely to 'nationalities.' Specifying in Article 5 that information 'on all nationalities' must be obtained therefore exceeds the requirements of the AMLRs, implying that obliged entities must ensure that customers disclose all their nationalities to them. The 'all' should accordingly be removed.

Furthermore, Art. 5 RTS should be aligned with Recital 3 RTS, which states that 'where a person holds multiple nationalities and declares them in good faith, verifying one nationality will be sufficient.'
Suggested alternative drafting:

Article 5 - Specification on nationalities (proposed new text in CAPITALS)

For the purposes of Article 22 (1), point (a)(iii), of Regulation (EU) 2024/1624 obliged entities shall obtain information on all nationalities or, where applicable, the statelessness and refugee or subsidiary protection status of the customer, any natural person purporting to act on behalf of the customer, and the natural persons on whose behalf or for the benefit of whom a transaction or activity is being conducted. WHERE A PERSON HOLDS MULTIPLE NATIONALITIES AND DECLARES THEM IN GOOD FAITH, VERIFYING ONE NATIONALITY IS SUFFICIENT.

Do you have any other comments on a specific article in the draft RTS?

- (●) Yes
- ( ) No

* Please state the article number in simple figures, without referring to the subparagraphs or points (e.g. '3' or '21')

Only values between 1 and 33 are allowed

6

* Please share your comments below, specifying the subparagraph and point, if applicable (e.g. paragraph 1 point (a)).

5000 character(s) maximum

Article 6 RTS – Documents for the verification of identity

Art. 6(5) RTS requires obliged entities relying on an identity document for verification to obtain either the original document or a certified copy thereof. However, it is currently common industry practice to rely on standard, uncertified copies of identity documents, which are then cross-referenced against other data sources. Mandating formal certification by a notary or public authority is a retrograde step that will introduce severe operational friction, high costs, and significant delays to digital onboarding processes. We therefore suggest deleting this requirement.

Suggested alternative drafting:

Article 6 - Documents for the verification of identity
5. For the purposes of verifying the identity of the persons referred to in Article 22(6) and Article 22(7), point (a), of Regulation (EU) 2024/1624, obliged entities shall obtain from that person the identity document, passport or equivalent, or a [DELETE] copy thereof, or act in accordance with Article 7.

Do you have any other comments on a specific article in the draft RTS?

- (•) Yes
- ( ) No

* Please state the article number in simple figures, without referring to the subparagraphs or points (e.g. '3' or '21')

Only values between 1 and 33 are allowed

7

* Please share your comments below, specifying the subparagraph and point, if applicable (e.g. paragraph 1 point (a)).

5000 character(s) maximum

We continue to be concerned by the lack of recognition of equally or more robust alternatives to electronic identification means that meet the requirements of Regulation (EU) No 910/2014 (Art. 22(6)(b) AMLRs), including in situations where these are either unavailable or cannot reasonably be expected to be provided. In the light of the anticipated difficulties in cross-border use of the EU Digital Identity Wallet, whether within or outside of the EU, availability of such an alternative becomes an ever more pressing issue. In this respect, the framing of Article 7 itself is too restrictive: Article 7(1) mandates the use of eIDAS as the primary means of verification, and the alternative provided in Arts 7(2)-(4) RTS is in turn limited to reliance on an official identity document. This precludes use of other available digital means of verification that may be less costly and more appropriate to the nature and risks of products offered (particularly where there is a low risk of identity theft). To use such alternative means is consistent with a risk-based approach, which suggests focusing resources on areas where they are most likely to prevent financial crime, as well as with the principle of technological neutrality, which has guided EU policy on remote onboarding to date.

This is particularly important given that financial crime evolves faster than any single technology can address: locking Level 2 around eIDAS as the primary modality embeds a technological bias into the AML/CFT regime and forecloses solutions that have demonstrated equivalent or higher assurance under the EBA Guidelines on remote customer onboarding (EBA/GL/2022/15). Furthermore, eIDAS is itself an identification instrument, not a ML/TF risk detection tool: it confirms identity at onboarding but does not address whether the customer is a

victim of identity theft, a money mule, under coercion, or whether the identity is a synthetic one generated through AI — risks that current verification solutions are specifically designed to detect. Mandating eIDAS as primary would therefore reduce rather than enhance risk-relevant information at onboarding.

In this context, it is important to note that it is now possible for information provided by a customer to be augmented with information available from reliable third-party sources and other signals that can be collected in real time during the onboarding process (including geographic indicators, online presence, etc.) These inputs can be ingested and validated holistically in a manner that allows for a better understanding to be obtained of a customer's identity and profile (and therefore potential financial crime risk) at a lower cost (which may be appropriate in the context of certain products), while also improving the experience for the customer. Overdependence on the submission of identity documents risks reducing the scope for further innovation in new identity verification measures and processes – to date, a notable strength of EU firms in comparison to peers in other regions – at a time when greater innovation and development in this space is possible now more than ever before.

As we have raised in our previous submissions, this issue is of great importance to FinTech firms because it: (i) impacts firms' ability to onboard new customers and thus their ability to scale their businesses, (ii) restricts their ability to employ innovative means of verification, (iii) impacts the costs of carrying out CDD, and (iv) disrupts the consumer journey, discouraging the taking up a payment product. One of our larger members estimates that they will incur an ongoing additional cost of 2.3M EUR per year given the manual review process that is required in instances when the user is not able to utilize an identification document that complies with a high level of assurance.

We therefore urge you to reconsider your approach to mandatory use of an official identity document. The RTS should explicitly recognise that in some circumstances a combination of customer-declared and implicit, programmatically collected data is a valid and proportionate basis for CDD, and that formal document verification is not required as a universal step in all cases.

Our members currently employ the following alternative means of verification. The RTS should allow flexibility for their use without prescribing any one means:

- Reliance on the funding account by establishing that a funding bank account with an EEA credit institution is in the name/control of the account holder;
- Database verification based on reliable credit and government sources;
- Cross-checks between digital footprint data (such as IP address, biometrics) and other elements of ID and of documentation, such as where the residential address is not stated on the official ID document; and
- AI/ML-based assurances.

Please see below for wording recommendations.

Do you have any other comments on a specific article in the draft RTS?

- (●) Yes
- ( ) No

* Please state the article number in simple figures, without referring to the subparagraphs or points (e.g. '3' or '21')

Only values between 1 and 33 are allowed

7

* Please share your comments below, specifying the subparagraph and point, if applicable (e.g. paragraph 1 point (a)).

5000 character(s) maximum

Furthermore, regarding Art. 7(4) RTS, we request clarification that the duty to 'justify' why the customer could not be verified through the means referred to under Art. 22(6) of Regulation (EU) 2024/1624 should be understood as a duty to 'explain' the use of an alternative means. This is to avoid the understanding that an assessment of any reasons supplied by a customer as to why they do not have e-IDAS compliant means of ID is to be made by the obliged entity (with the implication that some reasons may need to be rejected and onboarding consequently refused). The duty to explain should also be capable of being satisfied categorically (at a firm or product rather than individual customer level) where appropriate. For instance, where it is clear that e-IDAS compliant means are either not available or could not be expected to be produced, a detailed rationale for every customer would be inappropriate and serve little purpose. More fundamentally, Article 22(6) AMLR recognises both document-based and electronic identification as valid modalities, and a Level 2 measure should not narrow options recognised at Level 1; these further supports removing the per-customer justification requirement altogether.

Finally, to guard against a possible scenario in which pan-European uptake and interoperability of the EU Digital Identity Wallet does not fully materialise while alternative means of identity verification (as well as threats, such as those posed by AI-generated synthetic identities) develop at a continuing rapid pace, we recommend introducing a review clause in the RTS that will insure that requirements and assumptions that no longer reflect operational reality can be revised on a timely basis.

To give effect to the points raised above and to the principles of the risk-based approach and technological neutrality, the framing of Article 7(1) should be amended from 'shall' to 'may'. This restores eIDAS-based solutions as one valid high-assurance option without precluding other compliant remote verification solutions, aligns Level 2 with Article 22(6) AMLR and ensures that obliged entities retain the ability to choose proportionate measures of equivalent assurance, as the risk-based approach requires. The amendments to paragraphs 2 and 4, together with the review clause in paragraph 5, complete the calibration.

Suggested alternative drafting (changes in CAPITALS:

Article 7 - Verification measures conducted on a non-face-to-face basis

1. To comply with the verification requirements pursuant to Article 22(6) of Regulation (EU) 2024/1624 in a non-face-to-face situation, obliged entities MAY use electronic identification means that meet the requirements of Regulation (EU) No 910/2014 with regard to the assurance levels 'substantial' or 'high', or relevant qualified trust services as set out in that Regulation.

2. IN ADDITION, AND IN PARTICULAR in cases where the solution described in paragraph 1 is not available, or cannot reasonably be expected to be provided, obliged entities shall VERIFY THE NATURAL PERSON'S IDENTITY using remote solutions that meet the conditions set out in paragraphs 3 and 4.

3. Obliged entities shall ensure that the solution described in paragraph 2 uses reliable and independent information sources and includes the following safeguards regarding the quality and accuracy of the data and documents to be verified:
(a) controls to ensure that, WHERE AN IDENTITY DOCUMENT, PASSPORT, OR EQUIVALENT IS USED, the natural person presenting the customer's identity document, passport or equivalent is the person on the picture of the document;
[...]

4. Obliged entities using remote solutions shall be able to demonstrate to their competent authority that the remote verification solutions they use comply with this Article and they shall also be able to EXPLAIN, EITHER BY REFERENCE TO THE CUSTOMER OR THE OBLIGED ENTITY'S POLICIES, why the customer WAS NOT verified through the means referred to under Article 22(6) of Regulation (EU)2024/1624.

5. BY [DATE], AMLA SHALL, IN COOPERATION WITH THE COMMISSION, REVIEW THE APPLICATION OF ARTICLE 7 IN LIGHT OF THE MATURITY AND PAN-EUROPEAN INTEROPERABILITY OF ELECTRONIC IDENTIFICATION MEANS UNDER REGULATION (EU) NO 910/2014 AND SUBMIT A REPORT ACCOMPANIED, WHERE APPROPRIATE, BY PROPOSALS TO AMEND THIS REGULATION.

Do you have any other comments on a specific article in the draft RTS?

- (●) Yes
- ( ) No

* Please state the article number in simple figures, without referring to the subparagraphs or points (e.g. '3' or '21')

Only values between 1 and 33 are allowed

9

* Please share your comments below, specifying the subparagraph and point, if applicable (e.g. paragraph 1 point (a)).

5000 character(s) maximum

We would like to make AMLA aware of the fact that the second paragraph in Art. 22(3) AMLRs confuses the role of the issuing institution with that of the account servicing payment service provider ('ASPSP'). Art. 22(3) AMLRs requires the ASPSP to ensure that it can obtain information about the user from the issuing institution. However, given that the vIBAN user is the customer of the ASPSP in the first place and their identity has been verified by the ASPSP at the outset of the business relationship, the roles should be reversed, with the issuing bank required to ensure that it can obtain the information from the ASPSP. This should be clarified in the guidance.

Additionally, the wording in Art. 9 RTS 'shall obtain and verify' does not make the required distinction between the ASPSP, who verifies the identity of the vIBAN user, and the issuing institution, which is merely required to 'obtain information to identify and verify' (Art. 22(3) AMLRs). This difference in wording carries substantive implications: While the AMLR formulation permits reliance by the issuing institution on the verification undertaken by the ASPSP, the RTS formulation appears to impose an independent obligation to perform verification on the issuing institution. We suggest changes to the text below that highlight that distinction.

The additional obligations may very well lead to the loss of this very valuable innovation that is used by multiple PSPs for reconciliation of payments.

Finally, the meaning in Art. 9(c) RTS is uncertain, as it is not clear whether what is meant by 'the associated bank or payment account' is the underlying payment account that the vIBAN user holds with the ASPSP, the account that the ASPSP holds with the issuing institution or the vIBAN itself (which may in certain cases be re-used with another customer). This should also be clarified in the text of the guidance.

Suggested alternative drafting (proposed changes in CAPITALS):

Article 9 - Identification and verification of the identity of the natural or legal persons using a virtual IBAN

For the purposes of Article 22(3) of Regulation (EU) 2024/1624, IT IS UNDERSTOOD THAT the obliged entity THAT IS REQUIRED TO ENSURE THAT IT CAN OBTAIN INFORMATION ABOUT THE VIRTUAL IBAN USER FROM THE ACCOUNT SERVICING INSTITUTION IS THE ISSUING INSTITUTION. THE ACCOUNT SERVICING INSTITUTION shall obtain and verify the following information:

(a) In relation to the natural or legal persons using the virtual IBAN, the information required pursuant to Article 22(1) of Regulation (EU) 2024/1624;
(b) the virtual IBAN number assigned to that natural person or legal person;
(c) the dates on which the associated bank or payment account was opened and, where applicable, closed.

Do you have any other comments on a specific article in the draft RTS?

- (●) Yes
- ( ) No

* Please state the article number in simple figures, without referring to the subparagraphs or points (e.g. '3' or '21')

Only values between 1 and 33 are allowed

11

* Please share your comments below, specifying the subparagraph and point, if applicable (e.g. paragraph 1 point (a)).

5000 character(s) maximum

Articles 11 and 12 RTS – Corporate structures

We take issue with the requirement in Art. 11(4)(b) RTS for obliged entities to be satisfied that there is 'an economic, legal or other rationale' behind the ownership and control structure of a customer. This goes beyond the requirement in Art. 20(1)(b) AMLRs to 'understand' that structure, seemingly requiring a judgment of whether the structure is appropriate, necessary or justified. While requiring an understanding of a customer's ownership structure is sensible, anything more places too onerous a requirement on obliged entities and may result in unnecessary friction for legitimate multinational groups. It is also unclear how obliged entities could discharge their duty to comply with this requirement in practice and when a suspicious activity report would be required. We therefore suggest deleting this point, or minimally to provide a safe harbour' for listed or regulated group structures.

Relatedly, we think that the contributing factor in Art. 12(1)(b) of any part of the group structure being outside the EU for the structure to be considered 'complex' will catch too many legitimate (and in reality, non-complex) structures. Location itself should not be seen as contributing to complexity and therefore the risk of financial crime, unless the location is already designated as high-risk. Finding otherwise would impact the ability of European firms to offer services to customers that include in their structure an entity registered in, for example, the UK or US. We therefore suggest deleting this factor.

Suggested alternative drafting (changes in CAPITALS):

Article 11 - Understanding the ownership and control structure of the customer

4. When obliged entities assess the ownership and control structure, they must be satisfied that:
(a) the information included in the description pursuant to paragraph 2, point (a) is credible; AND [DELETE]
(B) that they understand how the overall structure affects the ML/TF risk associated with the customer.

Do you have any other comments on a specific article in the draft RTS?

- (●) Yes
- ( ) No

* Please state the article number in simple figures, without referring to the subparagraphs or points (e.g. '3' or '21')

Only values between 1 and 33 are allowed

12

* Please share your comments below, specifying the subparagraph and point, if applicable (e.g. paragraph 1 point (a)).

5000 character(s) maximum

Articles 11 and 12 RTS – Corporate structures

We take issue with the requirement in Art. 11(4)(b) RTS for obliged entities to be satisfied that there is 'an economic, legal or other rationale' behind the ownership and control structure of a customer. This goes beyond

the requirement in Art. 20(1)(b) AMLRs to 'understand' that structure, seemingly requiring a judgment of whether the structure is appropriate, necessary or justified. While requiring an understanding of a customer's ownership structure is sensible, anything more places too onerous a requirement on obliged entities and may result in unnecessary friction for legitimate multinational groups. It is also unclear how obliged entities could discharge their duty to comply with this requirement in practice and when a suspicious activity report would be required. We therefore suggest deleting this point, or minimally to provide a safe harbour' for listed or regulated group structures.

Relatedly, we think that the contributing factor in Art. 12(1)(b) of any part of the group structure being outside the EU for the structure to be considered 'complex' will catch too many legitimate (and in reality, non-complex) structures. Location itself should not be seen as contributing to complexity and therefore the risk of financial crime, unless the location is already designated as high-risk. Finding otherwise would impact the ability of European firms to offer services to customers that include in their structure an entity registered in, for example, the UK or US. We therefore suggest deleting this factor.

Suggested alternative drafting (changes in CAPITALS):

Article 12 - Understanding the ownership and control structure of the customer in the case of complex corporate structures

1. To understand the ownership and control structure of the customer in accordance with Article 20(1), point (b), of Regulation (EU) 2024/1624, obliged entities shall treat an ownership and control structure as a complex corporate structure where there are three or more layers between the customer and the beneficial owner and, in addition, more than one of the following conditions is met:
(a) there is a legal arrangement or a similar legal entity such as a foundation in any of the layers;
(b) [DELETE]
(B) there are nominee shareholders or nominee directors involved in the structure;
(C) the structure obfuscates or diminishes transparency of ownership with no legitimate economic rationale or justification.

Do you have any other comments on a specific article in the draft RTS?

- (●) Yes
- ( ) No

* Please state the article number in simple figures, without referring to the subparagraphs or points (e.g. '3' or '21')

Only values between 1 and 33 are allowed

18

* Please share your comments below, specifying the subparagraph and point, if applicable (e.g. paragraph 1 point (a)).

5000 character(s) maximum

Art. 18 RTS – Purpose and intended nature of the business relationship

We note that some of the information listed under Art. 18 RTS, particularly around estimated funds, anticipated transaction size and expected activity, will often not be meaningful information to collect as part of CDD for all firms in the same way it might be for a traditional bank.

In the FinTech sector many firms are new startup businesses that do not have a clear sense of what annual turnover they can expect to generate in the first year of operation or how quickly they might be capable of scaling up. In such cases, a declaration predicting turnover during onboarding may likely turn out not to be accurate or reliable, but this inaccuracy does not necessarily equate to elevated financial crime risk. We believe that in such circumstances other forms of benchmarking that do not rely on user input information (e.g., sector benchmarking against similar companies, forecasts based on price of goods sold, and other data) prove more reliable and can be utilised alongside ongoing monitoring, which generates objective behavioural data against which customer activity can be benchmarked in real time, are more effective risk controls.

A similar logic would apply to consideration of the destination of funds as touched on in Art.18(d) RTS, where the use of innovative payment methods and services might evolve or develop over time in a way that would not be seen in a traditional bank. In this case, as in the above scenario, we believe that methods of benchmarking, forecasting and monitoring that provide real-time insight and information will be more reliable and meaningful than estimates provided by users during CDD.

As such, we would be in favour of the RTS explicitly recognising – in either an operative provision or an additional recital – that firms should consider what information might be relevant to meeting the requirement of Art. 20(1)(c) AMLRs by applying a risk-based approach specific to their own particular business, and that in some cases alternative methods to those outlined in Art. 18 RTS might be appropriate.

Do you have any other comments on a specific article in the draft RTS?

- (•) Yes
- ( ) No

* Please state the article number in simple figures, without referring to the subparagraphs or points (e.g. '3' or '21')

Only values between 1 and 33 are allowed

30

* Please share your comments below, specifying the subparagraph and point, if applicable (e.g. paragraph 1 point (a)).

5000 character(s) maximum

Article 30 RTS – Sanctions screening

Article 30(a)(iii) refers to digital wallet addresses as identifiers for sanctions screening. However, wallet addresses are unlike names, which are clear in their given form and for which false positives are expected and managed. With wallet addresses, one cannot assume that what appears in a sanctions list is always a clean, canonical, chain-specific, valid 'address string' ready for deterministic equality checks. Before a match can even be identified, the data will need to be normalised (e.g., case-folding, checksum handling, prefix stripping, encoding format conversion) and malformed entries (e.g., truncated/partial entries, contextualised entries (e.g., "0x… (Ethereum)", "BTC: …", "TRON: …", labels, spaces, punctuation) will need to be addressed. The RTS does not provide a definition of whether a 'match' in this context means exact string equality or a match after normalisation and validation. This gap creates a risk of supervisory drift of expectation towards deterministic equality alerts with zero tolerance for any deviation in approach. This is ineffective in practice, as screening for deterministic equality will not contribute to the value of sanctions screening while it will make it harder for firms adopting a more realistic and appropriate approach to evidence compliant handling under Article 30(b) RTS

and timely processing under Article 30(d) RTS.

Suggested alternative drafting (changes in CAPITALS):

Article 30 - Screening requirements

For the purposes of Article 29, obliged entities shall:
(a) screen, through automated screening tools or solutions, or a combination of automated screening tools and manual checks, at least the following information on customers, beneficial owners and the entities or persons which control or meet the ownership conditions over such customers:
i. in the case of a natural person, all the names and surnames, in the original and/or transliteration of such data;
ii. in the case of a legal person, the registered name of the legal person, in the original and/or transliteration of such data;
iii. in the case of a natural person, legal person, body or entity:
– any other names, aliases or trade names where they differ from the registered name;
– digital wallet addresses, where available in the lists of targeted financial sanctions, AFTER THESE HAVE BEEN NORMALISED AND VALIDATED

Do you have any other comments on a specific article in the draft RTS?

- (●) Yes
- ( ) No

* Please state the article number in simple figures, without referring to the subparagraphs or points (e.g. '3' or '21')

Only values between 1 and 33 are allowed

31

* Please share your comments below, specifying the subparagraph and point, if applicable (e.g. paragraph 1 point (a)).

5000 character(s) maximum

Article 31 RTS – Risk factors for the electronic money exemption from CDD

We believe Art. 31 RTS introduces excessively restrictive risk factors that undermines the exemption in Art. 19 (7) AMLRs by unduly narrowing the scope of its application. We specifically recommend the following:

- Transaction Limits: Point (a) should be removed, as the AMLRs already set a low limit of EUR 150.
- Funding Sources: Point (b) requires that funds originate from an EEA-regulated account. This undermines the purpose of e-money as a cash substitute at points-of-sale and should be removed or extended to the SEPA area to allow, for example, travellers from the UK to take up an exempted product.
- Charges: Point (c) should be removed, as the charge for a product has no bearing on its ML/TF risk. This factor may also interfere with competition between providers.
- Geographical restriction: Products should be used to support the single market, and issuers should not be precluded from supporting such use; we therefore suggest that the geographical restriction in point (e) is removed and that the restrictions in points (j) and (k) are rephrased to countries outside the SEPA area.
- Distribution: We suggest deleting the references to ‘including electronic signature’ and ‘anti-impersonation’ in point (h), as specifying such CDD measures would go against the intention behind the exemption and undermine its use.
- Intermediaries: Point (i) should be removed, as it focuses on the distribution setup of the issuer rather than

the risk associated with the payment instrument itself and therefore falls outside AMLA's mandate.

Suggested alternative drafting (changes in CAPITALS):

Article 31 - Risk factors
Where supervisors decide to allow for an exemption under Article 19(7) Regulation (EU) 2024/1624, based on the conditions listed in Article 19(7), points (a) to (d), of Regulation (EU) 2024/1624, supervisors shall consider one or more of the following risk factors to determine the extent of that exemption:
(a) [DELETE]
(b) [DELETE]
(c) [DELETE]
(d) the nature and the range of the goods or services that can be acquired, including the level of risks associated with these goods and services;
(e) the extent to which the [DELETE] issuer is regulated by a national or regional public authority for specific social or tax purposes to acquire specific goods or services from suppliers having a commercial agreement with the issuer;
(f) the extent to which the transactions through the electronic money instrument are executed by an obliged entity that applies customer due diligence measures and recordkeeping requirements laid down in Regulation (EU) 2024/1624;
(g) the extent to which the payment instrument has a specific and limited duration in which the payment instrument can be used;
(h) the extent to which the payment instrument is available through direct channels which may include the issuer or a network of service providers and, in the case of online or non-face-to-face distributions, possess adequate safeguards [DELETE];
(i) [DELETE]
(f) the extent to which the payment instrument IS DISTRIBUTED OUTSIDE THE SEPA AREA [DELETE];
(g) the extent to which the issuer applies adequate technological tools, including geofencing and IP tracking, to restrict access from, transfers to or receiving funds from countries that are not WITHIN THE SEPA AREA [DELETE].

Do you have any comments on the recitals? The recitals are the statements at the start of the draft RTS and are numbered from (1) to (25).

- (●) Yes
- ( ) No

Please specify which recital you refer to, and share your comments below.

18

Do you have any comments on the Annex in the draft RTS?

- (●) Yes
- ( ) No

Please share your comments below.

Recital 18 RTS – Safeguarding accounts as correspondent relationships

The characterisation of safeguarding account relationships for Electronic Money Institutions (EMIs) and

Payment Institutions (PIs) as ‘correspondent relationships’ is unsupported by the definition of correspondent relationships in Art. 2(1)(22) AMLRs. A bank providing a safeguarding account to an EMI or EMI is not providing any services on behalf of the EMI/PI to its customers, as the account balance is owned by the EMI/PI. The banking services are therefore provided to the EMI/PI only.

Treating the provision of safeguarding accounts as giving rise to a correspondent relationship would impose onerous obligations on any EU bank providing such accounts to EMIs/PIs in third countries, including the UK, effectively requiring the safeguarding bank to assess the AML/CFT controls of the third-country EMI/PI (see Art. 36 AMLRs). This interpretation of the relationship, which has not been adopted previously and is neither expressed nor implied by the AMLRs, is therefore likely to exacerbate de-risking and create significant barriers to market access for non-EU institutions.

Suggested alternative drafting:

(18) This Regulation identifies a service that would benefit from specific simplified due diligence measures. This is the case where a credit institution opens a pooled account for a customer that is an obliged entity, to hold or administer funds that belong to the customer’s own clients, where the ML/TF risk of that service is assessed as low, based on the credit institution’s risk assessment. In such cases, since the final customers are already subject to the customer due diligence measures applied by the obliged entity, it is proportionate to allow specific simplified due diligence measures, in order to avoid duplication of controls while ensuring that appropriate safeguards remain in place. Situations where credit institutions open a payment account for payment institutions or electronic money institutions will fall outside the scope of the sectoral simplified measures provision of this Regulation. [DELETE]

Section 4 - Overall assessment

* How would you rate the proposals set out in the draft RTS overall?

- [ ] Inadequate
- [ ] Somewhat inadequate
- [x] Neutral
- [ ] Good
- [ ] Excellent

Would the implementation of the draft RTS generate any of the following additional costs beyond the adjustments that would be required to implement the rules set out in Chapter III of Regulation (EU) 2024/1624 (customer due diligence)?

This question is aimed at understanding the additional costs stemming from the implementation of these specific draft RTS, rather than the additional costs stemming from the provisions of Regulation (EU) 2024 /1624. We are interested in understanding the additional costs arising from the implementation of the draft RTS for your obliged entity. Please provide your responses with this context in mind.

For this survey, “costs” refer to the financial and resource implications your entity may face in implementing the draft RTS, including both initial setup efforts and ongoing operational commitments. Examples of one-off costs include amending policies and procedures, system upgrades, staff training or consultancy fees.

Examples of recurring costs may include additional reporting, monitoring, software subscriptions, or allocation of additional full-time equivalent resources, etc.

Please describe and substantiate the specific costs you foresee when implementing the provisions of these draft RTS.

	Manageable impact	Disruptive impact	No significant additional costs	Not applicable/no information available
One-off implementation costs	○	◉	○	○
Recurrent costs	○	◉	○	○

Thank you very much for your feedback.

Contact

Contact Form