# Your response has been received by EBA

Dear user,

Thank you very much for your interest in the European Banking Authority (EBA) and for submitting your comments to one of our consultations. Your response has been received and will be taken into account by the EBA. Please find below, for your records, the response you have submitted.

Please note that this email address is not monitored and does not accept replies. If there is something wrong or missing in your response to the consultation, please contact us at *eba.consultation@eba.europa.eu*.

Kind regards,

European Banking Authority

## Your answers are:

**Question 1: Do you have any comments on the approach proposed by the EBA to assess and classify the risk profile of obliged entities?**
With reference to Article 2 of the RTS – *Assessment and classification of the inherent risk profile of obliged entities* – we note that, as indicated in paragraph 3.2.1 of the consultation document (point 20(a)), the draft RTS does not include specific risk indicators or their respective weights. Additionally, point (9) delegates responsibility for developing related guidance to AMLA and competent authorities. This approach leaves obliged entities without the necessary clarity on how to define and apply risk indicators, thresholds, and weights, or on how to calculate inherent and residual risk. These elements are critical to ensuring a consistent and harmonised risk assessment framework and could serve as a reference for obliged entities' self-assessment methodologies. We therefore recommend further elaboration of point (9) to provide more detailed guidance.

Furthermore, it is essential that the data points required by AMLA under Article 12(7) AMLAR align with those requested by national supervisors under Article 40(2) AMLD. With option 2c selected, we are concerned that slightly divergent methodologies will lead to nearly identical - but still inconsistent - data sets. This would increase compliance burdens, especially if data must be submitted via different platforms (e.g., Excel for national supervisors, and a separate tool for AMLA), effectively doubling the reporting effort.

The proposed RTS represent a significant step toward achieving consistency in the assessment of inherent and residual risk profiles across Member States. However, we wish to highlight several concerns regarding their practical

implementation - particularly around data collection, timing, and system readiness.

Supervisors have already collected AML/CFT-related data from obliged entities in recent years, offering important lessons. Chief among these are the need for clear, consistent definitions and alignment of data requirements. The RTS introduce new data points that differ substantially from those previously collected. In many cases, obliged entities will need to adapt or develop internal systems, which requires time and resources.

Clear definitions are critical. Ambiguity in terms such as client type or transaction category risks divergent interpretations, undermining comparability and the reliability of risk assessments.

For group-level reporting, we seek clarification on:

- How to treat clients with relationships across multiple group entities;
- The treatment of intragroup transactions;
- Whether data consolidation should apply globally, within the EU, or only to EU-based obliged entities.

We also note the legal uncertainty surrounding AMLA's request for risk assessment data prior to the formal entry into force of the level 1 legal act. Article 40(2) AMLD mandates AMLA to draft RTS by 10 July 2026 but does not require them to be in force by that date. According to Article 78(1) AMLD, Article 40(2) will not enter into force until 10 July 2027, and it is not listed among the provisions with an earlier effective date. Therefore, any level 2 regulation under Article 40(2) cannot come into effect before July 2027, unless a specific legal basis for early application is provided.

Given the volume and granularity of the data required, sufficient lead time must be provided. The setup of systems and data quality controls will incur significant cost and effort. Reporting deadlines should reflect these operational realities. In particular, the annual requirement to assess and classify the risk profile of obliged entities by 30 September should be assessed for feasibility.

A phased implementation approach is essential to ensure feasibility. We recommend that a transitional period (soft-landing) is formally incorporated into the RTS, similar to the approach in the RTS on selection for direct supervision (see Recital 7). For the first two years after the RTS enter into force, data reporting should be treated as a best-effort obligation, allowing obliged entities to embed requirements and build necessary capabilities. A review after the first year should assess the relevance, burden, and clarity of the data points, allowing adjustments where needed. The implementation process should be seen as iterative, supported by ongoing dialogue between supervisors and obliged entities.

**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.**

We generally support the proposed relationship between inherent and residual risk - where residual risk may be lower, but never higher, than inherent risk. This distinction is particularly relevant for Groups, where centralised controls by one group entity may mitigate risks across subsidiaries. While assessments are done

on an entity basis before aggregation, a group-company may show significantly lower residual risk due to its broader mitigating role. (See our response to Question 8 on Art. 12(7) AMLAR RTS for further details.)

We note that while the RTS define required data points, national supervisors have discretion to determine how to collect them and may request additional information. This undermines harmonisation, especially for cross-border institutions, as reporting requirements may vary across Member States.

Finally, there is no clear provision for submitting supplementary information—particularly regarding internal controls and governance - nor is there any scope for dialogue with supervisory authorities. This limits transparency and could hinder accurate risk representation.

**3a: 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?**

We note that the volume of data points proposed—156 for Inherent Risk and 112 for Quality of Controls—is disproportionately high, especially considering the burden this would place on obliged entities (OEs) in terms of cost and operational effort. Data collection on products, services, and transactions will be particularly resource-intensive.

We recommend leveraging existing supervisory data return mechanisms wherever possible, incorporating relevant Annex I data points into these frameworks. This would help reduce duplication and operational strain.

We strongly advocate for a more **proportionate, risk-based approach**, in line with the Commission's simplification goals. In this context, **timing** is critical: with the first assessment expected in Q1 2027 based on 2026 data (per the EBA's public hearing on 10 April 2025), it is essential that the final list and definitions of data points be provided **as soon as possible in 2025**. System adaptations and reporting workflows require significant lead time. Indeed, not all required data is currently captured in separate system fields.

We urge the early publication of the interpretative note (referenced in Recital 19) to ensure clarity and comparability across Member States and obliged entities. Delays in providing clear definitions risk inconsistent implementation.

A key issue concerns the definition of "customer". Many banking systems are built around the "client relationship" rather than individual customers (natural/legal persons). This is especially true in private banking. Data extraction based on individual customers is currently unfeasible and adapting systems for this purpose would be extremely costly and time-consuming - likely impossible by 2026 or even 2027.

Additional clarification is needed for:

- The definition of customer (e.g. joint accounts, clients shared across branches, group-level structures);
- Transaction types included (e.g. whether fees or interest apply);
- Currency conversion (timing and method for EUR calculations - e.g. booking vs. reporting date).

We also propose that the data point *"Number of high-risk customers that are legal entities"* (Cluster 3.A) be removed from the controls section, as it pertains to inherent risk.

We seek further clarification on:

- Whether risk assessment results will be calculated for each OE on a stand-alone basis;
- Whether data will be collected only from stand-alone entities in each Member State;
- How the EU-level group risk assessment requirement applies when a financial group includes non-EU subsidiaries;
- How to treat assets booked in one jurisdiction but administered in another (both within and outside the EU).

The technical and operational changes that would be necessary for firms to provide all that is proposed to be required would likely come at very considerable cost for firms. These costs will vary widely and will depend on

- the size, scale, nature, and existing maturity level of reporting solutions within the obliged entity
- whether (and to what extent) the information is extracted currently
- whether (and to what extent) an obliged entity needs to design and build a bespoke solution
- the intended frequency and depth of supervision
- whether (and to what extent) the responses need to be derived from other data fields or can be directly extracted.
- whether (and to what extent) information is held in digital format or in multiple databases
- whether (and to what extent) data require cleaning before using
- whether (and to what extent) the systems of the obliged entity are compatible with that of the supervisor
- whether (and to what extent) relevant historical quantitative data or the data requested is retained by the entity in the form requested by the supervisor.
- Out of the 272 questions, we also suggest EBA identify a minimum set of core or critical data points / questions that obliged entities will need to provide during the first iteration of reporting.
- One financial institution with presence in minimum of six Member States in the EU has estimated high-level technology cost for building a solution based on two approaches.
- Cost estimate assumes that the data is available within the firm based on the RTS and interpretative guidance. Hence, collaboration only effort is required to source the data centrally.
- Assumes 40% of the work done within the firm by 2026 for existing EU jurisdiction specific reporting requirements can be reused.
- Changes will be required in multiple processes and systems to provide the information.
- Pre-requisite - Demographic and transaction data should be enriched (additional data points) to be able to produce the reports.
- New data sources need to be onboarded within the firm to provide response to certain sections.
- New transformation within reporting solutions to be created to prepare the data points as per the reporting requirement.
- Functional specifications to be updated.
- Cloud storage and compute costs for the data processing is added for one year and will be recuring henceforth.
- Enterprise Compliance Vault efforts.

<u>Option A:</u>

• Using the existing technology infrastructure

• Estimated cost includes building a reporting dashboard

Estimated Cost: 1.2 million USD*

Option B:

• Consider incorporating in-house AI solutions

• Estimated cost includes building an AI solution, reporting and relevant training required

Estimated Cost: 1.0 million USD*

*The above estimated costs include technology costs only and do not factor the compliance cost that will be required in addition.

In addition to the above factors which may impact the cost, assumptions made during the cost estimate...

**3b: 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 addition to the above factors which may impact the cost, assumptions made during the cost estimate

- Cost estimate assumes that the data is available within the firm based on the RTS and interpretative guidance. Hence, collaboration only effort is required to source the data centrally.
- Assumes 40% of the work done within the firm by 2026 for existing EU jurisdiction specific reporting requirements can be reused.
- Changes will be required in multiple processes and systems to provide the information.
- Pre-requisite - Demographic and transaction data should be enriched (additional data points) to be able to produce the reports.
- New data sources need to be onboarded within the firm to provide response to certain sections.
- New transformation within reporting solutions to be created to prepare the data points as per the reporting requirement.
- Functional specifications to be updated.
- Cloud storage and compute costs for the data processing is added for one year and will be recuring henceforth.
- Enterprise Compliance Vault efforts.

**3c: To what extent could the data points listed in Annex I to this Consultation Paper be provided by the non-financial sector?**
NA

**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.**
With reference to the provision stating that *"Supervisors shall carry out the first assessment and classification of the inherent and residual risk profile of obliged entities pursuant to Articles 2, 3 and 4 of this Regulation at the latest nine (9) months after the date of entry into force of this Regulation,"* we recommend that sufficient lead-time be allocated to obliged entities for preparation and data collection. We would recommend the review cycle aligns with the cycle of selection for direct supervision by AMLA (every three years).

This is particularly important in light of:

- the indication in Annex I that the final RTS will include an interpretive note clarifying sector-specific meanings of data points and associated dates; and
- point 19 of the Consultation Paper, which confirms that AMLA will not prescribe how data is collected, leaving this to national supervisors and acknowledging variation in data sources.

Until these clarifications are made available, obliged entities cannot reasonably begin the necessary operational planning or infrastructure development for data collection and submission. We therefore urge that the implementation timeline be adjusted accordingly to ensure feasibility and proportionality.

**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.**
NA

**Question 6: When assessing the geographical risks to which obliged entities are exposed, should crossborder transactions linked with EEA jurisdictions be assessed differently than transactions linked with third countries? Please set out your rationale and provide evidence.**
We support the proposal, as EEA jurisdictions generally maintain a higher level of regulation and supervisory controls - further reinforced by the AML Package - compared to third countries. This justifies the higher risk attribution to transactions linked to non-EEA jurisdictions.

**Question 1: Do you agree with the thresholds and 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.**
It should be clarified that these thresholds apply only to products that are physically offered within the relevant country. For example, if a German bank offers accounts to French residents through a physical presence or infrastructure in France, such offerings count towards the threshold. In contrast, cross-border products – such as an account held in Germany but accessible by a French resident – do not fall within the scope. Further clarification would be beneficial for specific cases, such as the treatment of virtual IBANs. A case can be made

for relative thresholds, as the materiality of activity is in relation to a) the member state's overall market size and b) the bank's size of operations.

The freedom to provide services is a core principle of EU law and is not subject to thresholds. However, the current proposal introduces the possibility of applying thresholds to this freedom as part of a de-risking strategy. Unlike the freedom of establishment, the freedom to provide services is characterised by the temporary nature of the activities. This essential feature, however, is not reflected in Article 1, which contains no reference to temporality. We therefore recommend adopting **cumulative** rather than **alternative** criteria to more accurately target the entities genuinely operating under the freedom to provide services.

Contrary to the statement made by the EBA during the public hearing on 20 April 2025, the initial selection process does not take into account transaction volume (TRX volume) per Member State - at least, this is not reflected in the wording of Article 1(1)(b) in conjunction with Article 12(7) of the AMLAR RTS. The limitation to a per Member State calculation is only explicitly mentioned in Article 1(1)(a), and solely in relation to the number of customers. In order to accurately calculate the transaction-value, clarification is needed as to which transactions are part of the calculation quantity for the transaction-threshold. E.g. are securities transactions; Nostro- and/or Vostro-transactions; or Forex-transactions included?

Relatedly, it remains unclear how the term "customer" is defined for the purpose of calculating the relevant threshold. Does the standard refer to contracting parties (i.e. natural or legal persons with whom the relationship is formally established), or to the ultimate beneficial owners of the assets - who, in the case of personal accounts, may be the same individuals?

The established thresholds are notably high, raising concerns about the potential exclusion of smaller yet high-risk institutions. We believe that AMLA should ensure that its direct supervision applies to a representative sample of obliged entities, particularly in terms of their size. However, the criteria used seem to limit the selection to large groups, which do not necessarily have the highest inherent risk levels. On the contrary, such groups have often made significant investments in strengthening their compliance frameworks, resulting in a generally lower residual risk.

Regarding the thresholds for the free provision of services, the two current thresholds appear excessively high: 20,000 clients or 50 million transactions under LPS. In relation with our previous commentary regarding the need to select entities of various sizes, the criterion consisting in the presence in six different countries seems excessive. Furthermore, the limit of 20,000 customers is inappropriate with regard to the different sizes of EEA member states. For example, this amount is nearly irrelevant for Germany (83 million people), but maybe significant for Malta (0,5 million people).

The selection method should indeed enable at least one institution per country but also ensure diversity in size and prevent the selection of only the largest establishments.

**Question 2: What is your view on the possibility to lower the value of the thresholds that are set in article 1 of the draft RTS? What would be the possible impact of doing so? Please provide evidence.**

For the reasons outlined above, we do not consider it appropriate, efficient, or effective to lower the thresholds. Doing so would merely result in a larger

number of obliged entities being included in the selection pool, thereby increasing compliance costs for those entities - without a realistic likelihood of being selected. Furthermore, we believe that lowering the thresholds is not appropriate in the context of temporary activities, which are characteristic of the freedom to provide services. Instead, we recommend introducing a risk-based factor linked to the provision of services in high-risk EU Member States - such as those listed by the FATF - as a more targeted and proportionate approach. As detailed in the response to the preceding question, we believe it would be prudent to lower these thresholds, as doing so, it would allow AMLA to directly supervise a representative sample of entities, particularly in terms of their size. This adjustment would ensure that supervision is not limited solely to large groups.

**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.**

It is unclear to us, why EBA is deliberating a distinction between retail and institutional customers, notwithstanding the lack of definition. If this is based on the desire to add some risk-based consideration to the selection process, it would be more appropriate in our view to distinguish between retail and private-banking customers.

Based on the assumption that the EBA subsumes any legal entity or arrangement under the term “institutional customer”, this would then also include operative small- and medium-sized enterprises, which would – from a risk perspective – be more suitable to be attributed to the retail sector; whilst retail clients (based on the assumption that the EBA largely considers individuals to be retail customers) could also be private banking clients.

Concisely, it depends on the intention of the distinction and the definition of the terms.

We propose a distinction between retail, corporate and institutional customers, as the associated activity falls into distinct categories of mass number of clients, accompanied by low average volume (retail), moderate number of clients, accompanied by high average volume (corporate), as well as low number of clients and mass volume (institutional), depending on the business model of a particular bank.

A distinction should also be drawn between natural and legal persons. In retail banking legal persons are riskier than natural persons. In wholesale banking corporates are riskier than institutional customers (most of them are regulated, which mitigates their risk). We therefore suggest a distinction between natural and legal persons.

This is because a differentiation must be made between natural persons (retail) and natural persons (wealth) and legal entities, given that natural persons (retail) generally present a significantly lower ML/TF risk. Retail customers’ behaviour is more homogeneous than that of institutional/corporate clients. The materiality of a single institutional client is usually much greater than that of a single retail client.

**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.**
We agree that the selection methodology should be based on the outcomes of the risk assessment conducted in accordance with the RTS on the assessment of the inherent and residual risk profile of obliged entities under Article 40(2) of the AMLD. As noted in our response to Question 3 related to the RTS under Article 40(2) of the AMLD, we recommend adopting a simplified and standardised approach to this methodology.

Additionally, we consider it essential that the RTS and/or subsequent technical documents should address the parametrisation and calibration methodology to provide more relevant weight to the inherent risk in the computation of the residual risk, as well as define a clear and transparent communication process for informing obliged entities selected for direct supervision by AMLA. This is crucial to mitigate potential stigma, which could adversely affect operations, including access to correspondent banking.

It is equally important to ensure that financial markets understand that such selection is solely for supervisory purposes and does not reflect on the soundness or stability of the selected entities.

**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.**
NA

**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.**
The methodology itself is congruent. However, it lacks the necessary detail in certain parts.

With reference to Article 5, point 2, we recommend providing clarification on the formula, supported by numerical examples to enhance understanding and ensure consistent application.

Moreover, we note that the methodology places more emphasis on quantitative data. However, the risk is not necessarily in the quantity: activities marketed to a small portfolio of clients may be high risk.

In our understanding, a shared client (for example, a client with both a banking and insurance relationship, where the bank is the holding and the insurance company the subsidiary of the holding) will be considered twice when calculating the risk score of the entity. For instance, a PEP client with a mortgage loan and credit balance insurance will, in this case, weigh twice as heavily. Logically, the criteria for shared clients within the same group should be taken into account.

**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.**

The scope of group entities covered by this exercise remains unclear, as does the role of the parent company in the collection and transmission of data points. To ensure consistency and avoid duplication, we recommend that the RTS provide clarification on the following points:

- Whether the assessment for identifying entities subject to direct AMLA supervision will be conducted at the group level, and whether it includes non-EU entities within the group.
- Whether the parent company is responsible for submitting data to AMLA on behalf of all in-scope entities, or if each entity - including those established outside the EU - must submit data individually. Regarding data collection and transmission, we support the EBA article requiring each relevant entity to report a questionnaire, with the authority responsible for aggregating the data. We also agree with the proposal that does not mandate the production of consolidated data points at the group level.
- Whether the parent company of a group with EU-based subsidiaries and foreign branches is required to report data to the group's home supervisor for those entities, even if they have already submitted data to their respective national supervisors.
- Whether the parent company must also report data on behalf of subsidiaries and branches located in non-EU jurisdictions to its home supervisor.
- Whether data related to foreign branches should be submitted separately or consolidated with that of the parent company.
- Whether data submissions may be made in different currencies or must be converted to Euro. Specification of the conversion methodology should be made. Further specifications should made defining transaction types in scope.
- Whether the parent company of the group located in a third country, with an EU branch, would be included in the scope of the group-wide perimeter. Further in such a scenario would the scope also then include other third country branches/subsidiaries of that same parent company. This clarification is important to determine whether the scope requires non-EU based undertakings to provide Annex 1 data to an EU-based supervisory authority in such a scenario.
- Furthermore, the factors (Art. 5(3)(i) to (iii) to Art. 12(7) AMLAR RTS) are not sufficiently determined to allow for accurate calculations. With regard to Art. 5(3)(iii) to Art. 12(7) AMLAR RTS, clarification should be provided as to what encompasses the "assets held or managed by the entity". For example, does this refer to client assets only? How should obliged entities deal with cross border-constellations with subsidiaries or the parent company in a third country?

Providing clear guidance on these aspects is essential to avoid duplication, ensure data consistency, and define responsibilities within cross-border group structures. Provision should be made for circumstances where foreign law does not allow for relevant data access or the delivery of reports to EU / Home regulators.

There are also concerns about the entities included in the group-wide perimeter: such as whether the entities of a non-EU group should be included. As this is a European regulation, it follows that only the European entities of the Group should be concerned. However, this approach would not reflect the entire intrinsic risk of the Group, which may arise from a presence in high-risk countries.

The scope of obliged entities needs to be clarified: does this apply only to entities subject to AML/CFT within a Group or also to non-subject entities? Cf. same comment for Art 40.

**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?**

We consider it appropriate to apply the same criteria to the parent company and other group entities when determining the group-wide risk profile. Once objective criteria for the risk assessment - including indicators and weights - are established, the parent company should be required to align fully with these, ensuring methodological consistency across the group. The proposed clarification under Question 7 above regarding non-EU based parent companies also applies here.

The weighting / consideration mentioned above depends on the operating/business model of the parent company. In the case of a financial holding with no clients, transactions or client assets, the ML/TF risk of the holding in practice is mostly comprised of the risk of its subsidiaries (i.e. none of the relevant factors of Art. 5(3)(iii) to Art. 12(7) AMLAR RTS are applicable). In the case of a financial holding with no clients, transactions or client assets, the contribution to the residual risk on a group-level, comes from the control environment of the parent, which might also cover inherent risks of the subsidiaries.

Subsequently it would be inappropriate to weigh the impact of the parent lower based purely on the factors of (i) number of customers; (ii) total transactions; and (iii) assets held or managed by the parent company.

The current model does not consider the performance of parts of the control environment by the parent or another group-company for that matter. It would need to be clarified that controls conducted by the parent contribute to the control framework of the subsidiary as well as the parent, as they would otherwise only be included in the residual risk on aggregated group-level with a substantially lower weight via the parent company due to possibly not fulfilling any of the relevance factors of Art. 5(3)(iii) to Art. 12(7) AMLAR RTS.

This is especially the case where the parent company performs additional controls for the benefit of the group-company. Due to the weighting based on relevance factors, these controls would not be taken into account adequately.

In the public hearing on 10 April 2025, the EBA indicated that a model whereby the parent performs parts of the controls for other group-companies would be regarded as outsourcing. We oppose this view strongly due to the fact that:

Outsourcing has a range of legal consequences; prerequisites and prohibitions of use (such as the notification to the supervisor (Art. 18 AMLR), contractual requirements, documentation requirements (Art. 9 AMLR), prohibitions in the context of risk assessment, approval of criteria for detection of suspicious or unusual transactions and activities (Art. 18(3) AMLR) and possibly further regulations based on Art. 18(8) AMLR) which are by no means intended and should not be applicable for the model in questions.

A score’s weighting is necessary for taking into account the relevance of each entity, as well as the risky activities within the entity. The aim is to avoid a dilution

of the risk favoured by a calculation model with only quantitative criteria. As mentioned in Question 6, the risk is not necessarily in the quantity: small entities may have a higher intrinsic risk than larger entities.

**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.**
NA

**Question 1: Do you agree with the proposals as set out in Section 1 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?**
**INDIVIDUAL CUSTOMERS**

1. **General remark: Missing clarity of targeted population**

Article 22 (1) of the AMLR requires obliged entities to obtain specific information to identify "the customer, any 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". Article 1 (1) of the draft RTS correctly cites Article 22 (1) AMLR but then sets out requirements only referring to "the customer", with no mention of the additional classes of persons set out in Article 22 (1) AMLR. It is unclear whether this is an oversight, or whether the EBA intends to target measures at a more limited population than that identified in the AMLR. However, in our view the latter is problematic, both from a practical perspective as well as from a risk perspective. For example, why should it only be permissible for obliged entities to ask a natural person customer to provide at least those names that feature on the customer's ID document but not a person purporting to act on behalf of the customer. These difficulties of interpretation with regard to the specific scope of application exist mutatis mutandis in Articles 3 to 6 draft RTS. Please refer to the more detailed table attached.

We therefore request that the following is clarified:

- Whether the reference in Art. 1 – Art. 6 draft RTS to a more limited population (of "customer[s]") than that cited in Article 22 (1) AMLR is an oversight, or a deliberate choice,
- The scope of the information to be obtained with regard to the identification of persons purporting to act on behalf of the customer[1], and of natural persons on whose behalf or for the benefit of whom a transaction or activity is being conducted, and
- Whether the requirements set out for "customers" similarly apply to the identification of
    - Natural person trustees of an express trust or persons holding an equivalent position in a similar legal arrangement, pursuant to Article 22 (1) (c) AMLR, and
    - Beneficial owners pursuant to Article 22 (2) AMLR, in combination with Article 62 (1) AMLR and/or also, where appropriate, to the identification of individuals as per Article 22 (1) (c) AMLR, in combination with Articles 57 to 60 AMLR.

## 2. **General Remark: Emphasising a risk-based approach and the purpose of data collection**

Recital Number 41 in chapter 3.2.3 of the draft RTS states that “the draft RTS adopts a principles-based approach in relation to the type and source of information to be collected by obliged entities but does not list specific documents”. This solely principle-based approach is questionable, not in line with the EBA’s own acknowledgements and objectives (see above), and will in many cases not lead to more efficient outcomes.

We generally have doubts whether this goes along with the explicit choice of a risk-based approach that the AMLR sets out in several places such as Art. 20 para. 2, Art. 25 AMLR (“if necessary”) and Art. 34 para. 3 and 4 AMLR. It is moreover explicitly introduced in recital Nr. 28 AMLR (“It is important that AML/CFT requirements apply in a proportionate manner and that the imposition of any requirement is proportionate to the role that obliged entities are able to play in the prevention of money laundering and terrorist financing”).

It furthermore could be understood to contradict FATF’s general call for proportionality and supporting of risk-based measures as set out in its guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing – High Level Principles and Procedures. FATF also aims at revising its standards to ensure countries apply a risk-based approach to their AML/CTF measures.

The principles-based approach outlined in the draft RTS potentially threatens to create further bureaucratic hurdles in the area of customer identification and the general fulfilment of customer due diligence obligations under the EU AML Regulation. This could further increase compliance costs for obliged entities and is not conducive to the goal of effective money laundering prevention. This contradicts the aim of reducing compliance costs and bureaucracy as also set out in the recital of the Draft RTS.

In light of this approach, the objective and purpose of some data remain unclear. For example, in addition to the above-mentioned Art. 10, it is not apparent how the registration of the country of birth as laid out in Art. 3 Draft RTS directly relates to effective AML prevention. Resolving this is highly critical, not only regarding the risk-based approach but also from a data protection point of view.

## 3. **General Remark: Additional Clarifications**

**Person purporting to act:**

In light of our members’ experience stemming from the implementation of Directive (EU) 2015/849 and Directive (EU) 2018/843), it would be sensible to limit the definition to third parties being natural persons and acting via proxy or power of attorney. In the context of wholesale banking, capturing individuals acting in their professional capacity (e.g., authorised signers), in particular those employed with regulated financial institutions, has proved excessively burdensome and ineffective in combatting financial crime.

We therefore suggest that a clear definition of a “person purporting to act” could be:

*legal representative(s) (e.g., legal guardians) of a natural person customer in situations where the customer is unable to act on their own behalf; any natural*

*person, other than an employee of a legal person authorised to act on behalf of a legal person customer pursuant to a mandate (e.g. an agent), or any natural or legal person authorised to act on behalf of legal person customers pursuant to a proxy agreement.*

This definition (or other similarly agreed definition) should be applied consistently across the AMLR and RTS.

**Refugees:**

We note that obliged entities shall obtain the statelessness and refugee or subsidiary protection status of their customer where applicable (Article 22 (1) a). However, the AMLR does not provide a definition of "refugee" and of "subsidiary protection status". We therefore emphasise that clarification (notably as to whether reference can be made to the EBA Guidelines and Statement on Asylum Seekers), and examples need to be provided, on what a refugee and status of subsidiary protection are.

**Information not to be found:**

Concerning information not to be found, we note that obliged entities are required to collect:

For a natural person,

- the national identification number, "where applicable", and the tax identification number, "where available", for the identification (Article 22 (1)).
- an identification document, such as a passport or equivalent for the verification and, where relevant, the acquisition of information from reliable and independent sources, whether accessed directly of provided by the customer (Article 22(6)).

For a beneficial owner,

- the number of identity document, such as passport or national identity document, and "where it exists", the unique personal identification number assigned to the person by the individual's country (Article 62 1. (a)).

We note the distinction made between the national identification number/the unique personal identification number and the identity document number. We request to clarify what kind of number is meant by the national identification number and the unique personal identification number. Do those terms refer to different numbers? What are the characteristics of /criteria for such numbers? Additionally, the various terminologies used to obtain these data ("where applicable", "where available", "where it exists") cause uncertainty.

Obliged entities are likely to encounter significant challenges in obtaining the national identification/unique personal identification numbers and the tax identification number as:

1. this information is not available in every country (e.g., Germany) and there is no comprehensive mapping of countries (EU or third countries) where such information exists
2. certain countries may impose restrictions on the cross-border sharing of this information (e.g., Belgium's for National ID number). Therefore,

regulator's expectation from obliged entities on the due diligences to be performed and proof of these diligences for obtaining these data is unclear.

We would therefore welcome clarification on the way to process when national standards do not permit the collection of the requested information. Can obliged entities rely on the customer's declaration that such number does not exist in their country of residence or cannot be shared?

In any case, the number of the ID document will be available through the copy of the document received. It is also important to precise that when a copy of the customer ID document has been obtained and filed, considering that the ID-number of the document is referenced therein, there should be no further request to file the ID-number in the information system. This would encourage heavy manual processes that can lead to errors.

We would also welcome clarification on the interpretation of "where applicable", "where available", "where it exists" provision in the regulation.

## 4. **Detailed comments on Articles 1 – 8, draft RTS**

### Article 1, Draft RTS – Information to be obtained in relation to names

We interpret Article 1 to require collection of full names and surnames as shown on the identity document.

We agree with the provision of collecting "those names that feature on their identity document, passport or equivalent", which is already market practice. However, it would be preferable to remove mention of "all of the customer's full names and surnames" which is confusing and can be contradictory. We therefore recommend revising Article 1(1) to state that "In relation to the names and surnames of a natural person as referred to in Article 22(1)(a) point (i) of Regulation (EU) 2024/1624, obliged entities shall obtain the natural person's names and surnames as featured on their identity document, passport of equivalent".

Suggested amendments to the article (words that are *italicised* are suggested to be removed, words in **bold** are additions):

Article 1(1) draft RTS

In relation to the names and surnames of a natural person as referred to in Article 22 (1) (a) point (i) of Regulation (EU) 2024/1624, obliged entities [*shall obtain all of the customer's full names and surnames. Obliged entities]* shall [**ask the customer to provide the names that feature on the relevant person's]** [*ask the customer to provide at least those names that feature on their]* identity document, passport or equivalent.

Clarity is needed on scenarios where the customer surname is not present. Whilst limited in occurrence, mononyms are used in certain circumstances.

For legal entities, the Article should clarify what the definition of "commercial name" is and whether the collection of it is mandatory or optional. Please note that in our view including the "commercial name" as a mandatory data field goes

beyond the requirements of the AMLR. However, we consider it relevant to collect the commercial name under a risk-based approach and at the discretion of the obliged entity, but only when it differs *materially* from the registered name. It should also be clarified that a commercial name is only in the collected documentation requested in cases where available; Art. 1 should be amended accordingly. Moreover, please be aware of the fact that the AMLR makes no use of the term “commercial name” or “trade name” which is used in Article 29. Article 1 (2) and Article 18 (1) (b) draft RTS refer to “commercial name”. Article 29 refers to “trade name”. We request clarity regarding the difference between those terms, if any. If “trade name” is intended to be synonymous with “commercial name”, we suggest that the RTS uses one term consistently. We request clarification of the term “commercial name” in an unambiguous manner.

We wish to draw attention to the fact that naming conventions vary across cultures and around the world. Similarly, passports and identification documents vary in the data points they provide, in accordance with the choices of the issuing authority. As such, the RTS should acknowledge this variability and allow a risk-based approach.

We also note that according to Article 18 draft RTS, the requirement to collect the commercial name shall also apply to other organisations (“…for a legal entity and other organisations that have legal capacity under national law…”). We assume that the requirements of Article 1 (2) draft RTS apply to these organisations by analogy. We would welcome confirmation of this assumption in the text of the final RTS by also including a reference to Art. 22 (1) (d), point (i), AMLR, to avoid any confusion or misunderstandings.

Regarding Art 29 (1) a) iii: Aliases and trade name: This implies an obligation to have this data in scope from targeted sanctions perspective. But the information is not mandatory CDD information under the AMLR. There is a need for clarification.

Suggested amendment to the article (words that are *italicised* are suggested to be removed):

Article 1(2) – “For legal entities, firms must obtain both the registered name, and where available, other alternate names [*, as applicable the commercial name where it differs from the registered name*].”

**Article 2, Draft RTS – Information to be obtained in relation to addresses**

We understand Article 2 to apply specifically to natural and legal persons as referred to in Article 22(1)(a) and (b) of the AMLR. It is unclear whether the same requirements apply to persons and entities mentioned under Article 22(1)(c) and (d), such as trustees or representatives of organisations with legal capacity or to the beneficial owners as well (see Art. 22 (2) AMLR).

Additionally, we recommend clarifying this in the RTS. We propose aligning the wording with EBA Guidelines EBA/GL/2024/11 (Travel Rule Guidelines), which require providing the “building number” or “building name” instead of building number and the apartment number.

We ask for more flexibility in situations where no postal code or street name exists. In such cases, institutions should be allowed to record the address as provided by the customer, consistent with Article 22(1)(a)(iv).. In those cases, and to ensure financial inclusion, we propose that the RTS should encompass flexibility. As to persons residing outside EU, we acknowledge that some

jurisdictions cannot provide postal code and/or street names to certain residential homes. In those cases, we support the need for flexibility while on the other hand it must be possible to provide data where the natural person is residing, e.g. by GPS coordinates.

We interpret “obtain” in this context to mean requesting the information from the customer, not verifying the address information.

Regarding residential address, the requirements are very detailed and therefore do not appear suitable for wholesalers, the customer’s representatives and UBO / SMO:

a. Requirements may not be necessary or appropriate for related parties in a wholesale context, where only the country of residence might suffice. The RTS should consider this distinction and provide flexibility accordingly.

b. Such extensive residential information of ultimate beneficial owners (UBOs) and senior managing officials (SMOs) are sensitive data points for corporate customers.

The sharing of certain details regarding the place of residence – particularly the street name – would increase the personal risk (e.g., kidnap risk, risk of other violence against the person) faced in particular by SMOs to an unacceptable level. In these cases, these individuals may prefer that their firms decline to enter into a business relationship, rather than provide the details requested. This would not be an efficient outcome and would harm EU’s competitiveness compared toother major financial markets which do not request this level of personal data. We therefore request to consider limiting the KYC data set at least for SMOs who are not beneficial owners (see recital 125 AMLR and recital 9 of the draft RTS). If SMOs are not the beneficial owners of a legal entity client there is no need for excessive KYC data sets in relation to this role.

The draft RTS only refer to the AMLR’s categories of natural persons and legal entities. We request that the RTS clarify if the obligations set out here are intended also to apply to trustees of an express trust or equivalent, other organisations that have legal capacity under national law, and beneficial owners.

Suggested amendment to the article (words that are *italicised* are suggested to be removed):

Article 2

The information on the address as referred to in Article 22(1) (a) point (iv) and 22(1) (b) point (ii) of Regulation (EU) 2024/1624 shall consist of the following information: the full country name or the abbreviation in accordance with the International Standard for country codes (ISO 3166) (alpha-2 or alpha-3), city, and where available other aspects of the address in accordance with the resident country conventions such as postal code*[, city,]* street name[*, and where available]* building number, building name and the apartment number.

We recommend that, besides the country and the city, all other information should be collected on a best-effort basis. Indeed, other information are heavy to collect, and if applied to all situations, the measure would be disproportionate with the benefits.

**Article 3, Draft RTS – Specification on the provisions of the place of birth**

In AMLR Art 22, obliged entities are required to obtain place and full date of birth cf. 22, 1, (a) (ii). In RTS article 3, EBA states that Place of Birth is defined as city and country. This goes beyond the legal requirement in the AMLR. The requirement also applies for BO. The consequence of this new requirement is that obliged entities must collect the new information, as details about the place of birth are not currently a legal requirement. This means that all customers will need to be contacted, and there is a need to develop IT systems to accommodate the new data point. This is costly and it also disrupts the customer experience. Furthermore, it is unclear what the information specifically adds to the verification and assessment process of a customer, and collecting data not used / relevant for effective ML/TF prevention purposes can be an issue in relation to the GDPR.

We believe the requirement to collect the country and city of birth should be limited to cases where this information is available. In practice, not all official identity documents include both the city and country of birth. It is our understanding that some official identity documents do not display any information related to the place of birth (such as Portuguese CNI). We therefore propose that it should be sufficient to obtain at least one of these two data points, with preference being the country, unless both are demonstrably required for risk mitigation purposes. We would further emphasise that nowhere in the Level 1 text is “place of birth” defined as country AND city; therefore, the RTS should allow for flexibility in terms of what components of place of birth are considered risk-relevant.

**Article 4, Draft RTS – Specification on nationalities**

We interpret the requirement to “satisfy themselves” that institutions must ask the customer to declare all nationalities held. We consider that this satisfies the declaration requirement, unless the institution has actual knowledge of contradictory information. In that case, further verification may be warranted. It should be noted that it is only possible to rely on the information provided by the customers / natural person.

To ensure clarity and consistency, it would be helpful if the article explicitly stated that institutions may rely on customer-provided information unless there are risk factors or red flags that would warrant additional verification. In our view, this would support a proportionate, risk-based application. Even in this situation, it is important to note that financial institutions will have very limited means, more often none, to challenge the client declaration. In any case, this requirement cannot be a result obligation.

Regarding the passage: “shall obtain necessary information to satisfy themselves that they know of any other nationalities their customers may hold”. This means that all natural persons to be identified under Art. 22 AMLR will need to be contacted, and there is additionally a need to develop IT systems to accommodate this data point. This is costly and disrupts the customer / natural person experience. Furthermore, it is not possible to verify a person’s nationalities or to ensure that all nationalities have been disclosed. The identification documentation provided which generally indicate only one nationality. There is no register, list, database or similar register or central record that contains the information and can be used for verification purposes.

As such, obliged entities must rely on declarations made by the individual.

We seek clarification as to the fact that information from the customer will suffice, unless the obliged entity has any reason to suspect an omission.

Otherwise, this raises a number of practical questions, such as:

- How will all nationalities be checked?
- How far should the investigation go? Should this information only be requested from the customer? We request clarification of whether Article 4 is intended to apply to the other classes of natural persons cited by Article 22 (1) AMLR, and to beneficial owners.
- If the client denies holding other nationalities, is no further action necessary?
- What if the client indicates possessing dual nationality, should the passport of the second nationality be requested? Can the onboarding/re-identification process not proceed until this passport is provided? What if this second passport is no longer valid?

We therefore believe that the wording of Article 4 requiring that obliged entities "shall obtain necessary information" is too far-reaching. We propose that the text of the provision is changed to "obliged entities shall ask customers to disclose any other nationalities they may hold".

It can be difficult to identify if a customer, a person purporting to act on behalf of the customer, or a beneficial owner has several nationalities. The identification of several nationalities is reliant on the natural persons, and a natural person to be identified might choose to disclose only one nationality. The bank cannot be held responsible when a natural person restrains other nationality information. We ask the EBA for clarification that obliged entities can rely on the declaration of the individual/natural person when obtaining all nationalities; it should therefore be specified that under a risk-based approach the obliged entity is only obliged to conduct further research if they have any indications of multiple nationalities (to the best of their knowledge).

A final question concerns why "statelessness and refugee or subsidiary protection status" are not mentioned in this article, but only in Art. 18 (SDD measures).

**Article 5, Draft RTS – Documents for the verification of the identity**

We interpret paragraph 1 of Article 5 as applying only to documents that are not official passports or **national identity documents** and understand that this Article establishes an exhaustive list of features that a document must contain in order to be treated as equivalent to a passport or national identity document for the purpose of verifying a customer's identity, in line with Article 22(1)(a) of the AMLR. The current list of conditions for an equivalent document is therefore too prescriptive: For example, in Sweden the driving license is used as an identity document but does not fulfil the requirements. This matter regarding the needed flexibility around the list of features an equivalent document must meet is critical, and we believe the list is currently too prescriptive. This is counter to the application of risk-based approach by obliged entities. For example, Drivers Licenses are an acceptable form of ID document industry-wide which are considered equivalent to a national ID/passport. However, these do not typically include nationality nor have a machine-readable zone (MRZ).

In particular, the requirement for a document to contain "biometric data" is problematic. It is unclear whether all identity documents from jurisdictions outside of the EU contain this data; it is questionable how obliged entities are supposed to verify this. Moreover, the "Biometric Data" condition where available

is impractical to verify whether in copy or an original document. This data is usually contained on an embedded microchip requiring an RFID reader to obtain. For face-to-face scenarios banks generally do not currently possess RFID reader technology to obtain this data and it is unclear how they would "verify" such. Requiring such would place an unreasonable – and, for the most part, unmeetable – burden on obliged entities at significant cost, particularly where other document features are sufficient to identify and verify the customer. For non-face to face scenarios, it would be impossible to obtain. The verification of ID-Documents by extracting information that is not displayed (visible without use of specialised tech) is generally a feature that has been implemented for the use of authorities and law enforcement, not obliged entities in the private sector. These boundaries should remain distinct. Where the document presented is a valid passport or national identity document issued by a state or public authority, we understand that this can be accepted without further conditions, even if certain elements listed in Article 5(1) are missing. For example, a passport that does not contain a MRZ does not have to be excluded from use if it is a valid government-issued identity document. This should not only be applicable to low-risk situations as mentioned in recital 14.

Similarly, with reference to Article 31(3) of the RTS, where e-wallets under e-IDAS are used, we assume that any missing attributes may be obtained and where necessary verified through alternative means.

Suggested amendments to the article (words that are *italicised* are suggested to be removed, words in **bold** are additions):

Article 5 – Documents for the verification of the identity

1. For the purposes of verifying the identity of the person in accordance with Article 22(6)(a) and Article 22(7)(a) of Regulation (EU) 2024/1624 a document, in the case of natural persons, shall be considered to be equivalent to an identity document or passport where all of the following conditions are met:

a. it is issued by a state or public authority,

b. it contains **the legal name (first and surname)** *[at least all names and surnames, the holder's]* date [*and place]* of birth *[and their nationality]*,

c. it contains information on the period of validity and a document number,

d. it contains a facial image and the signature of the document holder,

*e. [it contains a machine-readable zone]*

*f. [it contains security features and,]*

*g. [it contains, where available, biometric data]*

or – **a member state, in its legal system, considers that document valid for identification purposes.**

We assume that where the identity of a customer has already been verified under national legislation prior to the AMLR becoming applicable, this verification remains valid and there is no obligation to reverify a customer's identity merely because the document no longer meets all the conditions of Article 5(1) of the RTS. Once the identity has been verified, it should remain valid, unless risk-based triggers indicate a need for renewed verification. In this context, we note:

a) the consequence of this could be that a passport collected for verification measures at the time that is no longer valid should not result in a new

requirement to collect a new valid passport or equivalent, and

b) the need to demonstrate what is meant by risk-based triggers that indicate a need for renewed verification. The clearest examples are cases where the obliged entity becomes uncertain as to the identity of the customer, e.g. in cases of fraud etc.

Similarly, for Article 22(2) of the draft RTS, we assume that re-verification is not required.

In this context, it should be a requirement that the state or public authority must have verified the person's identity when the document was issued to a person/customer.

Staff will have to be trained to recognise authentic documents and detect forgeries. The draft mandates will likely increase the administrative load and compliance costs for the bank. It is important that EBA considers this in its draft RTS and seeks effective yet resource efficient solutions.

In line with recital 7, we strongly emphasise the need for flexibility in accepting identity documents for customers such as refugees or persons from jurisdictions where standardised identity documentation is not widely available. In such cases, we consider that institutions must retain the discretion to determine equivalence on a case-by-case basis, based on its source, reliability and the specific context. It may be useful to consider whether certain clear categories of public servants and/or employees of NGOs could verify the identity of homeless and other vulnerable categories of customers in order to support the aim for financial inclusion.

Regarding paragraph 2, we would also support clarification what legitimate reason means (e.g. only written for the vulnerable, those that would otherwise be excluded, or does it need to be understood more broadly? Shall the interpretation be limited to cases of asylum seekers or persons in similar situations, as the example given in Recital 7 draft RTS may suggest?). It is our understanding that legitimate reasons encompass both location-based circumstances (such as countries in a state of war) and individual circumstances (such as homelessness or legally protected adults).

It shall be noted that a birth certificate used to identify minors when they do not have an ID document / passport / equivalent yet would not fulfil the listed requirements. Consequently, accounts for minors could not be opened in such cases.

Article 5(3) to the Art. 28(1) AMLR RTS states that OEs shall take reasonable steps to ensure that all documents obtained according to Article 22(6)(a) and Article 22(7)(a) AMLR are authentic and have not been forged or tampered with. We seek clarification as to the interpretation that such measures are only necessary if there are doubts about the authenticity of these documents; and what constitutes “reasonable steps” regarding identity documents issued by authorities according to Article 22(6)(a) and Article 22(7)(a) AMLR. Article 7 of to the Art. 28(1) AMLR RTS also requires for a reliability and independence check regarding the information sources used. We seek clarification insofar as this obligation generally only applies to third party sources and does not refer to documents issued by authorities such as identity cards.

Regarding paragraph 4, certified translations should not be mandatory where the institution can reasonably determine the content of the document through other means, such as (online) translation tools or existing internal expertise.

Obligation to take reasonable steps to ensure authenticity;

Paragraph 4 requires obliged entities to take "*reasonable steps*" to ensure that documents are authentic and have not been forged or tampered with. There is no known source of expertise or central register to verify every possible document issued by every possible global public authority. In the absence of such, we request that the EBA clarify what would constitute obliged entities taking "*reasonable steps*", as used in this context.

Regarding paragraph 5, the terms "provide" and "certified" require further clarification, particularly in the context of remote or online onboarding. We interpret the term "provide" to mean that the customer must make the identification document available to the obliged entity, either in person or through secure digital means in line with Article 6, including digital uploads in secure portals; and that "certified" be defined in a way that reflects practices in both physical and digital certification.

Additional clarification is needed regarding the acceptability of a simple vs. certified copy. Article 5 (5) draft RTS states that obliged entities must see an original identity document, passport or equivalent, or a certified copy thereof, or must verify in accordance with Article 6. It is unclear if obliged entities can accept simple copies if verified through other sources, in keeping with the risk-based approach, or if only certified copies are deemed acceptable for verification of identity. We request that the EBA clarifies if simple copies can be used for this purpose.

Finally, additional clarification is requested regarding the acceptability of certified copy provided by client vs. received from notary / qualified lawyer. We would request clarification as to whether a certified copy can be received directly from the relevant person, or if the certified copy must be received directly from the relevant notary / qualified lawyer. It is common practice, especially in the UK and the US, that certified copies can be produced by company secretaries i.e. not necessarily a qualified lawyer or notary. It is important that an obliged entity is able to certify as well.

---

[1] We would define the "person purporting to act on behalf of the customer" as "any natural person authorised to act effectively on behalf of the customer vis-à-vis the obliged entity." We request that the RTS explicitly define "any person purporting to act on behalf of the customer". It should clarify whether this definition includes only third parties acting via proxy or power of attorney, or it if also encompasses authorised signers and senior managers.

---

**ULTIMATE BENEFICIAL OWNERS**

**Article 9, Draft RTS – Reasonable measures for the verification of the beneficial owner**

Article 22 (7) (b) of the AMLR delineates the methods for verifying the identity of the beneficial owner, one prescribed method is: “by taking reasonable measures to obtain the necessary information, documents, and data **from the customer** or other reliable sources, including public registers other than the central registers.” In the current draft of Article 9 of Draft RTS, among the reasonable measures for beneficial owner identity verification, there is no mention of collecting data directly from the customer (this provision is only referenced in Article 19 of Draft RTS when applying simplified due diligence measures). Since AMLR permits the collection of information from the customer irrespective of the applicable due diligence level, the RTS should not contravene the flexibility granted by the Regulation and include the provision of information from the customer as an additional source for verification.

When verifying the beneficial owner based on public registry, the full set of information required by Art. 62(a) of Regulation 2024/1624 is not available (e.g. number of ID document, nationality). Accordingly, we can only rely on information as available from those public registries. We suggest adopting a similar criterion as provided under RTS section 1, art. 5, paragraph 2, for those scenarios, namely: name, surname, place of birth, date of birth, together with Tax code (or equivalent, social security number).

In addition, we ask to consider to explicitly include credit agencies and/or comparable data services providers as another example for reliable sources that can be used for verification purposes under Art. 9 (b) draft RTS. According to our experience such credit agencies are widely used in practice as they provide a good and reliable data quality.

We also need clarification on the basis for such data sharing “[…] up-to-date information from credit or financial institutions as defined in Article 3(1) and (2) of Regulation (EU) 2024/1624, which confirm that the beneficial owner has been identified and verified by the respective institution […]”.

We fully support the measure requiring the use of certain local and EU registers, notably the tax register and passport database. These registers are currently not accessible in all EU countries, we hope that these databases will become accessible to obligated entities.

**Article 10, Draft RTS – Understanding the ownership and control structure of the customer**

(1) The extensive requirements needed in order to understand the ownership and control structure of the customer in cases of complex structures go beyond the wording of the AMLR. Furthermore, the current wording of Art. 10, Draft RTS, contradicts the risk-based approach promoted by the AMLR in not giving the option of less strict information collection in a low-risk scenario. According to our understanding, the reference in Art. 20 (1) lit b AMLR to “take reasonable measures” clearly introduces a risk-based approach when it comes to the verification of the beneficial owner’s identity and the understanding of the ownership and control structures. Taking into account the specific circumstances of each legal entity client and their concrete ML/TF risk involved, the wording of the AMLR leaves room for obliged entities to decide whether and if yes which concrete information on intermediate beneficial owners they deem necessary to collect to proportionately fulfil the requirements of Art. 20 (1) lit. b AMLR. Art 10, Draft RTS does not reflect this appropriately and we explicitly request to include a reference to the risk-based approach by inserting the exact wording from Art. 20 (1) lit. b AMLR “take reasonable measures”. The starting point for the assessment of obliged entities whether and which additional information on

intermediate beneficial owners within the ownership and control structure are sensible to obtain from an AML/CTF perspective should always be an organigram of the structure provided by the legal entity customer. However, compliance with the requirement to understand the ownership and control structure does not necessarily require an examination of the entire structure of the legal entity customer by the obliged entity. Once again, a risk-based approach regarding the scope of the reasonable measures taken should be allowed. In this context, it is our understanding – and confirmation would be welcomed - that the requirements set out in Art. 10 (1) lit. (a), Draft RTS, are met by obtaining such an organigramme/organisation chart, and that no further obligation is introduced by the wording “intermediary connections”. Clarification on the meaning of term “reference” used would also be welcomed (i.e. does it mean the name of the intermediate entity?). We also seek clarification as to the fact that this is an examination along the ownership chain and does not refer to the entire structure of the beneficial owner.

(2) We consider the requirements under Article 10(1) lit. b and c, draft RTS, to be extensive and to go beyond the requirement to understand the ownership and control structure. Any information on intermediate entities prescribed within the RTS to Art. 28 AMLR should be relevant to (1) adhere to the requirements set out in Art. 20 (1) lit. b AMLR, i.e. the requirement to understand the customer’s ownership and control structure and to know who the beneficial owner of a legal entity customer is and (b) from a ML/TF risk perspective. Obliged entities should therefore not be required to collect identical data and information regardless of the risk classification of the business relationship. In addition, please keep in mind that even Art. 62 (1) lit. d AMLR which is not relevant for the KYC process of obliged entities but clearly addresses only legal entities, trustees etc. required to notify beneficial ownership information to the Central registers does not require to obtain the overly broad range of data about intermediary connections as proposed in Art. 10 (1) lit b and c, Draft RTS. However, Article 10 (1) lit. b & c, Draft RTS even require information such as legal form, reference to the existence of any nominee shareholders, jurisdiction of incorporation or registration and the sub-division by class or type of shares and/or voting rights for each legal entity part of the structure that are also not explicitly required under Art. 62 (1) lit. d AMLR.

Overall, the proposed requirements do not seem to be sufficiently risk-based and would impose a significant burden on obliged entities, particularly those dealing primarily with other financial institutions or similar intermediaries where the customers would in almost all cases have a control structure containing more than one legal entity or legal arrangement. Consequently, this would have a large impact in terms of related costs and would render the establishment of business relationships and the ongoing due diligence more complex.

We therefore strongly recommend aligning the RTS with the AMLR’s scope and providing clarification on how institutions can obtain this information efficiently. Insofar, it should also be kept in mind that obliged entities do not have an own business relationship with intermediate entities within the ownership and control structure of a customer and have therefore only limited options to obtain any information on intermediate entities at all. In line with the risk-based approach, obliged entities should be required to establish the ownership structure and only identify intermediary layers where there are concerns around the legal/economic rationale for the structure.

We propose to insert the following limitation in lit b of Art. 10 (1), Draft RTS (*italicised* text is suggested to be removed):

b. with respect to each legal entity or legal arrangement [*within the referred ]*functioning as intermediate beneficial owners [*intermediary connections]*, the

legal form of each legal entity or legal arrangement, [*and reference to the existence of any nominee shareholders]* where needed to ultimately understand the ownership and control structure; the jurisdiction of incorporation or registration of the legal person or legal arrangement, or, in the case of a trust, the jurisdiction of its governing law and; where applicable, the shares of interest held by each legal entity or legal arrangement, [*its sub-division, by class or type of shares]* and/or voting rights expressed as a percentage of the respective total (if different from shares of interest), where beneficial ownership is determined on the basis of control, understanding how this is expressed and exercised.

We request the deletion of Art. 10 (1) lit. c. Please note that the information for listed entities is already publicly available. There is no use in the collection of such data from an effective ML/TF prevention perspective. As this information for listed entities is already publicly available, such requirement would be an unnecessary collection exercise of data that is already publicly available.

(3) Article 10 (2), Draft RTS in addition requires obliged entities to assess if the information obtained on the ownership structure is “plausible” and if there is “economic rationale behind the structure”. Once again, we are of the opinion that this assessment requirement, which shall also apply even in low-risk situations where SDD is applied (i.e., once again, the risk-based approach is not properly reflected), goes beyond the requirements of Article 20 (1) (b) AMLR. Understanding the ownership and control structure does not necessarily include an own assessment whether the structure is plausible, and an economic rationale is behind it. Neither Art. 62 nor Art. 63 AMLR, which only addresses legal entities etc. and their own notification requirements towards the Central Registers and are therefore not relevant for the KYC process, do require such an assessment.

We therefore request to delete Art. 10 (2), Draft RTS in its entirety. In addition, we consider it unclear by what means an obliged entity is able to assess the “plausibility” of the information on the ownership structure as provided by the customer and how to demonstrate compliance with this requirement. We recommend clarifying and providing concrete examples of how to meet such requirements provided that Art. 10 (2), Draft RTS shall be kept. We would then also appreciate a clarification about what is meant by “description” (i.e. an organisational chart?)

We suggest that the text of this Article be redrafted to focus on understanding the ownership and control structure of customers, particularly in complex and higher-risk situations, as follows (*italicised* text is suggested to be removed):

For the purposes of understanding the ownership and control structure of the customer in accordance with Article 20(1) (b) of Regulation (EU) 2024/1624, where the customer’s structure appears unusually or excessively complex given the nature of the customer’s business, and may pose a higher risk of ML/TF [*and in situations where the customer’s ownership and control structure contains more than one legal entity or legal arrangement]*, obliged entities shall take reasonable measures to obtain where necessary the following information:

a. [*a reference to all]* the names of the legal entities and/or legal arrangements functioning as intermediary connections between the customer and their beneficial owners that are relevant for the determination of the beneficial owner and which own or control a substantive share of the customer structure, if any;

b. with respect to each legal entity or legal arrangement within the referred intermediary connections, the legal form of each legal entity or legal arrangement, and [*reference to the existence of any nominee shareholders*;] the jurisdiction of incorporation or registration of the legal person or legal

arrangement, or, in the case of a trust, the jurisdiction of its governing law [*and; where applicable, the shares of interest held by each legal entity or legal arrangement, its sub-division, by class or type of shares and/or voting rights expressed as a percentage of the respective total, where beneficial ownership is determined on the basis of control, understanding how this is expressed and exercised.]*

*[c. information on the regulated market on which the securities are listed, in case a legal entity in an intermediate level of the ownership and control structure has its securities listed on a regulated market, and the extent of the listing if not all the legal entity's securities are listed on a regulated market.]*

If the suggested deletion of (c) set out above is not accepted, then we suggest at least reducing the scope of the requirement to the ultimate parent, as follows (*italicised* text is suggested to be removed):

c. information on the regulated market on which the securities of the ultimate parent are listed, in case the ultimate parent *[a legal entity in an intermediate level of the ownership and control structure]* has its securities listed on a regulated market, and the extent of the listing if not all the ultimate parent legal entity's securities are listed on a regulated market.

2. Where warranted by the facts of the situation at hand, obliged entities shall assess [*whether the information included in the description, as referred to in Article 62(1)d of Regulation (EU) 2024/1624, is plausible, there is economic rationale behind the structure, and it explains how the overall structure affects the ML/TF risk associated with the customer]* whether a structure might have been set up only in order to avoid or reduce the transparency of beneficial ownership, with no other likely or possible legitimate justification apparent.

**Article 11 of the Draft RTS – Understanding the Ownership and Control Structure of the Customer in Case of Complex Structures**

We find the definition of "complex structure" overly broad. Many international clients naturally have multiple ownership layers across jurisdictions. Applying this definition without a risk-based assessment could lead to unnecessary burden and the outcome that most structures must be considered as being complex (which is not justified under an effective ML/TF perspective). We recommend allowing for proportionality and risk-based judgment. It is, however, understood that a complex structure does not automatically lead to enhanced due diligence (EDD) (even though it is considered a high customer risk factor, pursuant to the 2025 FATF Recommendation 10) due to the wording in AMLR Article 34. The objective should be to identify situations where a company's shareholder structure appears unusual or excessively complex in relation to the company's activities. The definition of complex structure should then be revised to align with this aim. Confirmation of this assumption would be helpful.

We request that the removal of a mandatory definition of "complex structures", as setting one-size-fits-all criteria will result in a tick-the-box exercise that is not informed by real ML/TF risks. Article 11 should allow obliged entities to apply a risk-based approach in setting up specific internal procedures to identify appropriate criteria for complexity. If this is not possible, as a fallback option, we recommend deleting points a) and c). With respect to point b), we suggest adding the following specification: "(...) different jurisdiction in high-risk third countries pursuant to Article 29 – 31 AMLR", also considering an extension of the concept of "high-risk countries" under the AMLR. We consider this approach is consistent with Rationale 41, which highlights the need to follow a risk-

based approach that focuses on effective outcomes to avoid an increase the cost of compliance without tangible benefits.

Suggested alternate wording:

Article 11 – Understanding the ownership and control structure of the customer in case of complex structures

To understand the complexity level of the ownership and control structure of the customer in accordance with Article 20(1)(b) of Regulation (EU) 2024/1624, obliged entities shall establish adequate policies and procedures specifying the criteria that make ownership and control structures complex for the business relationships for which the obliged entity provides products and services.

The criteria should include factors such as, but not limited to:

1. the number of layers between the customer and the beneficial owner that may be an indicator of complex ownership structure

2. the high-risk third countries in which these entities are incorporated or domiciled, if any

3. indications of non-transparent ownership with no legitimate economic rationale or justification and

4. the presence of known nominee shareholders and / or directors that are involved in the structure.

**Article 12 of the Draft RTS – Senior Managing Officials (SMOs) under Article 22(2) of the AMLR**

Article 22(2) of the AMLR provides that senior managing officials (SMOs) must be identified in cases where no beneficial owner can be determined, or where there are doubts concerning the identity of any beneficial owners previously identified.

However, SMOs are not, in fact, beneficial owners – as acknowledged in recital 125 of the AMLR and recital 9 of the Draft RTS to Art 28 AMLR. While the EBA states that the same information should be collected for SMOs as for beneficial owners, the AMLR is silent on the question of what kind of data obliged entities shall collect for a proper identification of SMOs. Even if not directly stated, the EBA's approach appears to imply that the information required under Article 63 (4) of the AMLR should also apply the identification and verification requirements regarding SMOs within the KYC process of an obliged entity. However, this is not the case as Art. 63 only addresses legal entities and their requirement to submit beneficial ownership and/or SMOs' information to the Central Registers.

We believe that if the legislator had intended SMOs to be treated in all respects as beneficial owners within the KYC process of an obliged entity, this would have been clearly prescribed in Article 22(2) of the AMLR. This is not the case as Art. 22 (2) AMLR merely requires obliged entities to "identify" SMOs. By mandating, in Article 12(a) of the draft RTS, that full information in line with Article 63 (4) AMLR be collected on SMOs, the EBA arguably exceeds its mandate, extending obligations in a manner not foreseen by the AMLR.

The proposed approach under Art. 12 Draft RTS also raises questions about the purpose of collecting such detailed information from an effective money laundering prevention perspective: since SMOs are not de facto beneficial owners, they cannot act as such. Therefore, collecting extensive data under Article 63 (4) AMLR – which is directed at legal entities but not obliged entities – appears to lack practical meaning in this context and may not be in line with GDPR requirements.

Moreover, we have already highlighted the challenges involved in gathering the full range of information required under the AMLR from all beneficial owners. Extending these requirements to SMOs is likely to exacerbate these difficulties, potentially leading to adverse consequences for customers without demonstrably improving risk management.

To ensure a harmonised and proportionate application of Article 22(2) of the AMLR, the EBA should instead provide clearer guidance on what constitutes a “sufficient basis” for identifying an SMO. In our view, the business address should suffice for senior managing officials (SMOs). Requiring a residential address is disproportionate and adds limited value. Similarly, nationalities and place of birth of SMOs are not necessary for identification purposes. We believe that name and date of birth, plus business address, are sufficient to identify SMOs within the KYC process and meet the intention of the legislator. There should not be a verification requirement.

Furthermore, Article 22 (2), AMLR, states that “Where, after having exhausted all possible means of identification, there are doubts that the persons identified are the UBOs, obliged entities shall record that no UBO was identified and identify all the natural persons holding the positions of senior managing officials in the legal entity and shall verify their identity”. Due to the requirements under Art. 21 AMLR, it is unclear in which cases an obliged entity knowing that a prospect or a client conceals the identity of its real UBOs can enter into or maintain a relationship. To ensure a harmonised and proportionate application of Article 22(2) of the AMLR and as distinct from Art. 21 AMLR, the EBA should also provide clearer guidance on what constitute “doubts” and the steps a bank should take when there are doubts regarding the identity of the UBO of a (potential) client.

Further points that we would note regarding SMOs are:

1. The RTS should include a specific reference whether the definition of SMO under Art. 63(4) AMLR hall also apply for the KYC process (“senior managing officials” means the natural persons who are the executive members of the management body, as well as the natural persons who exercise executive functions within a legal entity and are responsible, and accountable to the management body, for the day-to-day management of the entity).[1] We assume that this is the case. However, we then request clarification who is meant by the second half sentences “natural persons who exercise executive functions within a legal entity and are responsible, and accountable to the management body, for the day-to-day management of the entity”). The definition seems to be very broad and appears to cover every first management level function below the management board / board of directors of a legal entity. Such an extensive interpretation would have a considerable impact on obliged entities and customers, particularly large corporate customers;
2. With reference to art. 22, par. 2 of the AMLR we would highlight that some passages are not clear and need more clarification. We refer, in particular, to the following:

"*Where, after having exhausted all possible means of identification, no natural persons are identified as beneficial owners, or where there are doubts that the persons identified are the beneficial owners, obliged entities shall record that no beneficial owner was identified and* ***identify all the natural persons*** *holding the positions of senior managing officials in the legal entity and shall verify their identity".*

Without prejudice to the wording of the provision, it would be necessary to evaluate the possibility of proceeding with a "gradual" identification of these subjects, on the basis of the role actually exercised. A different approach would have a considerable economic impact.

**Articles 13 and 14, Draft RTS – Identification and Verification of Beneficiaries of Trusts**

We suggest clarifying what constitutes "sufficient information" under both articles, e.g. by providing practical examples, especially for complex trust structures or where information is not publicly available.

Art. 13(2) to the Art. 28(1) AMLR RTS state that obliged entities shall take risk-sensitive measures to ensure that the trustee, the legal entity or the legal arrangement provide timely updates, including on specific events that may lead to beneficiaries previously identified by class or characteristics becoming ascertainable and thus beneficial owners.

It is unclear how this requirement should be transposed into practice. Generally speaking, the "risk-sensitive measure" to address changes in circumstances, that have not been made known to the obliged entity, is the risk-based review and ongoing monitoring of business relationships. According to Art. 26(3) AMLR it is necessary to review a business-relationship outside the normal review cycle under certain circumstances, including the legal obligation to contact the customer for the purpose of reviewing any relevant information relating to the beneficial owners in the course of the relevant calendar year.

The periodic and ad hoc (in case of change of circumstance and the "2011/16/EU"-) - review is the measure of choice for the ongoing monitoring of a business-relationship. The review is the risk-based measure that has the best cost-benefit ratio in terms of ongoing monitoring. It is important not to overload obliged entities with administrative measures that are no longer risk-, but rule-based (without adding a substantial benefit); as this approach leads to a quantitative increase in checks which take attention and resources away from adequate, effective and qualitatively suitable measures.

In Article 14(2)(b), we recommend adding the word "reasonable" before "measures" to reinforce that a risk-based approach is permitted, as this aligns with the principle of proportionality and existing AML/CFT practices.

Moreover article 64, p. 3, AMLR provides that trustees shall "*provide the information on the beneficial owners and on the assets of the legal arrangements that are to be managed in the context of a business relationship or occasional transaction to obliged entities when the obliged entities are applying customer due diligence measures in accordance with Chapter III*".

Accordingly, Articles 13(2) and 14 (2)(b) Draft RTS should be amended to recall that this obligation falls primarily on the trustee – and not on obliged entities - who must also fulfil it promptly.

We would also welcome examples of what “specific events” requiring an update are.

---

[1] We note that if the definition of SMO is the same as the one in Article 63, this would capture a very large number of natural persons. We request a more targeted interpretation, in line with the risk-based approach: only individuals who exercise actual executive power.

**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.**
**Article 6, Draft RTS – Verification of the customer in a non-face-to-face context**

Generally speaking, in relation to Art. 6 Draft RTS “Verification of the customer in a non-face-to-face context”, we would highlight that is not very clear why e-IDAS compliant solutions are first choice and the other solutions a “second best” just in case the first solution is not available or cannot reasonably be expected to be provided. Regarding this point we would like to highlight that banks have recently – and costly – implemented remote on boarding solutions compliant to EBA guidelines that needs to be maintained not just a second solution but equal to the e-IDAS compliant solution. Moreover, accordingly to the current figures, solutions adopted in line with the EBA guidelines on remote boarding solution are proofed more effective, than e-IDAS compliant ones, to prevent fraud.

We suggest the EBA consider proportionality and practicality in these cases, allowing a risk-based approach when verifying documents that do not naturally contain advanced security features. While we acknowledge the importance of secure identity verification, the current drafting risks creating rigid, operationally challenging requirements that may undermine customer experience and limit the flexibility of obliged entities to tailor their onboarding process. It would be greatly beneficial to clarify that a non-face-to-face context is not a requirement for the use of e-IDAS instead of a passport.

Specifically, Article 6(1) makes the use of e-IDs at a “substantial” or “high” level of assurance or qualified trust services mandatory, if such means are available. This requirement is unnecessarily restrictive and inconsistent with Article 22(6) AMLR, which does not impose a mandatory obligation to use such tools. In practice, e-IDs and qualified trust services can introduce frictions into the onboarding process due to redirects or non-responsive systems, potentially resulting in higher drop-out rates. Moreover, the practical functioning of the EU Digital Identity Wallet is still unclear, particularly in cross-border non-face-to-face context, making a meaningful comparison with other remote verification methods premature.

Suggested amendment:

Article 6 (1) draft RTS

To comply with the requirements of Article 22(6) of Regulation (EU) 2024/1624 in a non-face to face context, obliged entities shall **apply specific and additional measures to compensate the potentially higher risk that this type of customer relationship presents, or may** use electronic identification means, which 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.

Finally, with respect to the first paragraph, we request further definition of what the use of “relevant qualified trust services as set out in that Regulation” means.

Regarding Article 6(3), we request further guidance on what is meant by “this consent must be recorded”, specifically, what form of recording (written, electronic, audio/video) is considered appropriate and sufficient. Additionally, the purpose of the consent is ambiguous: consent under EU law must be freely given, implying a real alternative. If no fallback process is provided, the consent becomes de facto mandatory. This may reduce transparency for the customer and lead to meaningless, default consent similar to those seen in cookie policies. It should also be clarified whether such consent may be withdrawn, and if so, what the consequences are for verification and account access.

Article 6(5) appears inconsistent with the context of non-face-to-face identification. If the original document is not presented physically, features such as holograms cannot be examined as indicators of authenticity. We recommend clarifying how institutions are expected to assess such security features in practice.

Article 6(6) requires clarification on how institutions are expected to demonstrate compliance with the obligation to “examine the security features of the document.” In many cases, especially when onboarding international legal entities, obliged entities rely on copies of foundational documents. These will lack security features and may not lend themselves to authenticity verification without access to external databases or tools not readily available.

There is a need for confirmation that an e-ID meeting the necessary e-IDAS requirements can also be used in a face-to-face situation with a customer, as well as a passport can be used.

Premature reliance on e-IDAS and the current exception should not be limited to situations where e-IDAS is unavailable or cannot be reasonably be provided. Furthermore, it is unclear which cases exactly fall under “unavailability” and “cannot reasonably expected to be provided”.

Rationale:

According to Article 28 AMLR, RTS shall be developed on the information necessary for the performance of CDD including on the reliable and independent sources of information that may be used to verify the identification data of natural or legal persons.

Regulating (various) verification methods is extremely important, in particular through video legitimation or other new remote verification methods (e.g. account ID system used in the Netherlands) that comply with the EBA Guidelines on the use of Remote Customer Onboarding Solutions and the Article 13(1) of Directive (EU) 2015/849, since they model the most consumer-friendly and inclusive version of a verification for remote onboarding. This is even more important since it ensures access for all categories of customers to banking

services and banking products (including those that belong to vulnerable groups and / or live in rather remote cities with few bank branches. Without this option and the broad acceptance of other methods next to electronic identification means which meet the requirements of Regulation (EU) No 910/2014 and/or are relevant qualified trust services as set out in that Regulation the (digital) opening of accounts would be very restricted.

We would further suggest that the future RTS provides a few concrete examples of digital systems, which allows obliged entities to use a variety across the EU such as the Account ID system which other EU countries already use. Additionally, we would like to point that there is currently no specific mention made of the possibility to rely on e-IDAS protocol “substantial” level solutions. We therefore propose that national digital ID solutions that comply with the assurance level “substantial” (or higher) of the e-IDAS protocol should be seen as sufficient for verification of all customers, including customers with a high-risk profile. The RTS should explicitly allow such an approach.

*Third paragraph*: need for explicit consent is questionable and clarification on the type of consent is required.

**General remark**:

It is our understanding that obliged entities may decide on their own with which verification methods and documents they verify the KYC data sets for legal entities, trusts, legal arrangements (including Trustee and any person holding an equivalent position) and other organisations that have legal capacity under national law.

For legal entities, the identification and verification process should rely on official commercial registers or equivalents.

The constitutional documents of a company, legal arrangement or foundation (articles of incorporation, company constitution etc.), when drawn up in accordance with relevant law, should also be considered as an adequate source to identify and verify a legal entity. The RTS should confirm this position / interpretation.

In addition, we understand that obliged entities are also allowed to use other sources for verification purposes as long as they adhere to the requirements for assessing the reliability and independence of a source pursuant to Art. 7 draft RTS. Confirmation of this understanding would be welcome.

We seek clarification with regards to the validity of authentication on documents pursuant to Art. 9(b) to Art. 28(1) AMLR RTS issued by attorneys, notaries, and other public bodies (e.g. courts, notaries). We are of the opinion that based on equivalent regulation of such counterparties said authentications should be considered suitable pursuant to this standard.

In our understanding, the financial institution will be required to provide an e-IDAS-compliant tool (if available) and another similarly robust online verification solution (in line with the EBA guidelines) in cases where the customer cannot provide an e-IDAS-compliant electronic identity. In our opinion, the RTS only consider online means of onboarding, while many financial institutions still maintain agencies where clients can be identified and verified physically (offline).

We would like to see reflected in this article a choice: the financial institution should provide an e-IDAS-compliant solution and/or a similarly robust online verification solution for banks that offer offline onboarding (onboarding in an agency).

The rationale is that requiring the provision of both an e-IDAS-compliant tool and a similarly robust online verification solution (in line with the EBA guidelines), in addition to an offline onboarding system (in an agency), would be excessively costly for financial institutions, significantly increasing the costs of compliance. Offline verification in an agency remains a sufficiently accessible mechanism that protects vulnerable individuals.

As a general comment it will be practically challenging and costly to develop new systems for remote identification, such as video conferencing or selfie verification system.

**Article 7, Draft RTS – Reliable and independent sources of information**

We consider that the reference in Article 22(6)(a) AMLR to the use of reliable and independent sources "where relevant" should be interpreted as only relevant where an identity document, passport or equivalent is not available. This implies that in most cases it will not be necessary to acquire additional information beyond the identification document to verify the customer's identity. We interpret this in a such a way that if the identity documentation is sufficient, there is no obligation to obtain other identity documentation from reliable and independent sources.

Further clarification is needed on what constitutes "risk-sensitive measures to assess the credibility of the source."[1] The current language leaves room for different interpretations, particularly regarding what level of due diligence is expected for different risk categories.

We consider that a customer declaration (when there is no contradictory information) can fall within the scope of a reliable and independent information in lower-risk scenarios, when applied as part of a broader risk-based approach.

The comparison of KYC requirements in various EEA Member states found that misalignments exist in respect to the acceptable "age" or "up-to-datedness" of legal entity data and the supporting documentation which is used for the KYC review. Differences not only exist in respect to the acceptable timespan since an evidentiary document was issued (ranging from six weeks to three, six or even 12 months), but also in respect to the reference date which is used to determine the end-date of this period. Here, some regulators define the age of a document as "at time of receipt by the financial institution", whereas others require that data and documents cannot be older than a given timeframe "at the time of the sign-off" (completion) of the review. Time-limits linked to the completion date frequently cause issues, for example when UBO-information has to be obtained from foreign shareholders, whereas shorter "age-period" restrictions negatively impact banking groups which serve a legal entity customer on a pan-European level as it time-restricts the group-internal "portability" of the KYC customer file between countries.

We therefore ask for clarifications – not only for reasons of proportionality - that the "age of the document" is tied to "time of receipt by the financial institution" as well as standards on how to deal with publicly registered and accessible documents, e.g. from the commercial register.

We suggest giving a clear definition of the "end-date" of the period in relation to verification documents where such a "time-stamp" seems to be sensible (e.g. documents obtained from an official register or another official source), ideally as "not older than [x] months at time of receipt by the bank", rather than "not older than [x] months at time of sign-off and completion of the review" to avoid the

need to refresh data or documents during the ongoing KYC review process. In relation to other documents, it should be clarified that obliged entities are allowed to use a risk-based approach when it comes to the validity question of documents.

We request an explanation how to assess the potential risk of forging: how can obliged entities perform such assessments. Moreover, this goes beyond the ML/TF topic and includes a fraud aspect. It has a significant cost for the obliged entity to manage this assessment while it should also be explained how this assessment should apply.

---

[1] We note that this is the only place in the RTS where the term “credibility” is used. In all other instances, “reliability” is used. For consistency reasons, we would propose using “reliability” uniformly.

**Question 3: Do you have any comments regarding Article 8 on virtual IBANS? If so, please explain your reasoning.**
**Article 8, Draft RTS – Identification and verification of the identity of the natural or legal persons using a virtual IBAN**

Generally, there are questions regarding identification and verification of identity using a virtual IBAN where the PSP is not in the EU and not bound by EU law. This could, by implication, potentially mean that the EEA-Bank cannot do business with a non-EEA PSP.

The Financial Action Task Force (FATF) is currently processing feedback received to its consultation on changes to Recommendation 16, which concerns payment transparency. The FATF consultation focused on ensuring that the account number or payment message data which are transmitted as part of a transaction can identify the financial institution and the country where the funds are held. FATF is expected to publish the results of its consideration of feedback in June/July 2025 – which will coincide with the EBA considering feedback received to this consultation. We request that to the extent possible, the EBA consider aligning the final requirements of Article 8 with final changes to Recommendation 16. Global alignment is helpful in ensuring effective compliance and reinforces the benefit of FATF’s work to set standards at the global level.

We would ask EBA to specify what information on the identity of the natural or legal person shall be obtained. Furthermore, from the wording of paragraph 3 of Article 22 AMLR, second paragraph, it is not clear whether such information must always be obtained or only upon request.

Under Article 22(3) AMLR the banks servicing the bank or payment account to which a virtual IBAN issued by another credit or financial institution redirects payments are required to obtain the information to identify and verify the identity of the natural or legal persons using any virtual IBAN from the institution that issues the virtual IBAN without delay and, in any case, within five working days.

In view of Article 22(3) of AMLR and Article 8, Draft RTS, it would be critical to understand the different roles identified in these articles. For that reason, we ask first and foremost clarification on these roles (i.e. “credit or financial institution

servicing the account", "issuer of a virtual IBAN", "entity that provides a virtual IBAN to a person" and "user of a virtual IBAN").

**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?**
**General remarks:**

According to our understanding of Art. 20 (1) lit. c) and Art. 25 AMLR obliged entities are not required to take all the actions set out in those Articles in all instances. Rather, obliged entities are allowed to apply their judgement and take certain action only in certain circumstances, in accordance with a risk-based approach.

The drafting of Article 15 and 16 draft RTS does not sufficiently reflect the risk-based approach evident in the AMLR. These provisions set out an extensive list of requirements that appear to disregard the necessity for proportionality and risk-sensitivity, particularly in normal risk situations. We recognise that the text refers to "risk-sensitive measures". It is not however clear in the text of the draft RTS that obliged entities should first assess whether the measures need to be applied at all. We advocate that the text of the RTS will be amended to appropriately reflect the risk-based approach which can be clearly derived from the AMLR. We do not see the need for collection of all the information listed in Articles 15 and 16 for normal CDD.

In addition, where the purpose and intended nature of the relationship or transaction is evident from the products and services themselves, there should be no requirement to collect any further information. This simplification should at least apply to low-risk situation where SDD is applied.

The granular nature of the information to be obtained under these Articles leaves little to no room for obliged entities to apply discretion based on the actual identified level of ML/TF risk. In cases where there are no risk indicators and a customer poses a normal risk, requiring such extensive data collection is neither proportionate nor effective. Rather, it creates unnecessary friction in business relationships with well-intended customers, negatively impacting customer experience and diverting resources from higher risk cases. It might also warrant unnecessary client outreach even when the purpose and intended nature can already be inferred from the product and existing or intended relationship.

For example, the requirement to obtain detailed information on a customer's employment income (including salary, wages, bonuses, pension or retirement funds, government benefits, business revenue, savings, loans, investment income, inheritance, gifts, and other asset disposals) is excessive in the absence of any risk indicators. In a normal CDD context, this information does not contribute meaningfully to the risk assessment or the understanding of the business relationship. Such data collection should only be triggered where the nature of the relationship or transaction raises specific concerns that warrant further investigation. This also contradicts the GDPR-principle of data minimisation (Art. 5(1)(c) EU 2016/679 "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

Similarly, the expectation to collect information about the expected type(s) of recipients, jurisdictions of incoming transactions, and comprehensive details about the customer's occupation (including the sector, industry, operations, products and services, regulatory status, geographic footprint, and revenue

streams of the employer) is disproportionate for a natural person opening a payment account or engaging in routine transactions and is not in line with Art. 5(1)(c) EU 2016/679.

Institutions should not be expected to implement the same level of measures for occasional clients as they do for regular clients with whom they maintain a business relationship.

**Article 15, Draft RTS – Identification of the purpose and intended nature of the business relationship or the occasional transaction**

Regarding Paragraph c: We request the deletion of "wider group" and limiting the information sharing requirement to cases where relevant, as pursuant to Article 16 (3) of the AMLR, the obligation to share information among obliged entities within the group is confined to instances "when such sharing is relevant for the purposes of customer due diligence and money laundering and terrorist financing risk management". This provision acknowledges that not all customer information is deemed relevant, thereby permitting a risk-based approach to information sharing this goes beyond the AMLR requirements. The question otherwise arises of what shall be done in relation to secrecy locations (e.g. Switzerland, China)?

In line with above, we suggest the following amendments:

c. **where available**, whether the customer has additional business relationships with the obliged entity's **group**, and the extent to which that influences the obliged entity's understanding of the customer and the source of funds, **provided that obtaining this information does not conflict with other regulatory rules and requirements.**

Article 15(d), which stipulates that obliged entities must determine the source of wealth where the ML/TF risk is higher, also raises concern. Even within the context of EDD, determining the source of wealth should not be a standard requirement (see our comments to Article 27). It is an intrusive measure that should be applied selectively and only in clearly high-risk scenarios. Treating it as a standard obligation in any higher risk context is counterproductive and inconsistent with effective risk prioritisation. We request to delete "source of wealth" only required for EDD as per Article 25 AMLR. Article 15 draft RTS only refers to Article 20 (1) (c) AMLR.

We therefore request that Article 15 (1) (c) draft RTS be deleted – or if this should not be accepted, then amended to read:

whether the customer has additional business relationships with the obliged entity or its wider group, and the extent to which that influences the obliged entity's understanding of the customer and the source of funds, **provided information sharing is permitted and not in breach of confidentiality, data protection and use of information**; and [...]

**Article 16, Draft RTS – Understanding the purpose and intended nature of the business relationship or the occasional transaction**

Regarding Paragraph d: We request the deletion, or – alternatively – the clarification, the wording "information on the expected types of recipients" in relation to the destination of funds, as it is unclear whether it relates to the legal form of the recipients or to other elements.

Regarding Paragraph e:  it appears to be difficult to obtain this information – the overall scope of information in line with the risk involved and under due consideration of Art. 5(1)(c) EU 2016/679.

As currently drafted, we believe Articles 15 and 16 read more as a template for EDD in high-risk situations and not as a proportional and risk-based framework for standard CDD. We urge the EBA to revise these Articles in line with the risk-based approach and allow obliged entities the opportunity to tailor their information collection based on actual risk. Article 25 of the AMLR already defines what information must be obtained and assessed to understand the purpose and intended nature of the business relationship. Expansion beyond this without clear high-risk indications undermines the principle of proportionality. For normal risk customers/normal CDD, we propose to apply a proper risk-based approach, in accordance with the principle of proportionality.

**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?**
**INDIVIDUAL CUSTOMERS**

**Article 17(1) of the RTS**

We are of the view that a more proportionate, risk-based approach should apply to relatives and close associates (RCAs) of PEPs, taking into account the nature of the relationship and the individual's risk profile. Furthermore, the RTS should explicitly confirm that obliged entities are not required to obtain from each identified PEP a comprehensive list of all family members and close associates. Imposing such dual requirement would be both impractical and excessively intrusive.

**Article 17(2)** appears to indicate that only **automated screening tools and measures** are required to identify PEPs, implying that direct questioning of the customer is not necessary. We request confirmation that obliged entities are not required to explicitly ask customers about their PEP status. According to the draft RTS, PEP screening should be conducted on a risk-based basis and at a minimum when relevant changes occur in the customer due diligence data and PEP lists. Preliminary risk factors include the nature of the customer's business, employment, or occupation, among others. We interpret this to mean that re-screening is required when there is a change in relevant customer data and PEP lists. In practice, PEP screening is primarily carried out by matching customer data (first name, last name, date of birth, and place of birth) against PEP databases. We therefore propose that this obligation should not be extended to other elements.

**ULTIMATE BENEFICIAL OWNERS**

**Article 17, Draft RTS, Treatment of Senior Management Officers (SMOs) Identified as PEPs**

The exposure of beneficial owners to politics and political decision making may entail a heightened risk of financial crime. However, SMOs – who do not own assets, control resources, or offer or stand to benefit from political influence to the same extent as beneficial owners – do not pose equivalent risks.

Applying the same measures to individuals who pose a lower risk as those who present a higher risk would be an inefficient use of resources and would divert attention away from the most significant sources of risk. We request that the RTS clarify this, as well as the appropriate steps required when identifying SMOs as PEPs, specifically when no UBOs have been identified.

**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?**
**SIMPLIFIED DUE DILIGENCE FOR INDIVIDUAL CUSTOMERS**

**Article 18 of the RTS**

In practice, obliged entities apply varying definitions and categorisations of customer risk levels. It would therefore be helpful if the final RTS acknowledged this diversity in approach. The RTS should clarify that “low(er) risk situations” encompass any situation that is not classified as “high risk”, and that all customers not assessed as high risk – including medium risk - are generally eligible for simplified due diligence measures under Section 4.

Regarding the place of birth, the country should be sufficient if the city is not available in the official document.

Regarding the indication of “Other nationalities,” the obliged entity shall ask the customer if they have multiple nationalities and can only rely on the customer’s own declarations. In practice, the obliged entity will often be unable to verify the accuracy of a client’s claim to hold only one nationality. It should not be required to actively search for undeclared nationalities unless there are specific reasons to suspect that the customer holds multiple nationalities from a risk-relevant perspective (e.g. in the case of U.S. citizenship automatically granted based on the place of birth in the United States). In the context of simplified due diligence, the obliged entity should therefore be required to collect only one nationality. It is worth noting that, for the purpose of screening against targeted financial sanctions lists, the most relevant data point is typically the customer’s name (see our comments on Section 6).

It would also be advisable to provide for the possibility of deferred verification in the RTS, as is currently allowed in certain EU countries.

Regarding the definition of "person purporting to act on behalf of the customer," we propose clarifying that this term refers to "any natural person authorized to act effectively on behalf of the customer vis-à-vis the obliged entity."

We suggest that Article 18(b) draft RTS be amended to read as follows (*italicised* text is recommended to be deleted):

For a legal entity and other organisations that have legal capacity under national law, the legal form and registered name of the legal entity [*including its commercial name]* and where available other alternate names, in case [*it differs]* these differ from its registered name; the address of the registered or official office and the registration number, the tax identification number or the legal entity identifier where [*applicable]* available.

**Article 23 of the RTS**

We consider that the reference to understanding the source of funds in this Article is not aligned with Article 20(1)(f) AMLR, which treats the source of funds as part of ongoing monitoring and only “where necessary”. In low(er) risk situations, the purpose and intended nature of the business relationship should primarily be derived from the type of product or service the customer obtains from the obliged entity. There is also no basis to require source of funds information by default. Doing so would undermine the risk-based approach and the concept of SDD.

**ON-GOING DUE DILIGENCE FOR INDIVIDUAL CUSTOMERS**

On **Article 22 of the RTS**, we interpret this to mean that in low-risk situations - i.e., where there are no indicators of high risk (and not only in SDD cases) - the obliged entity may rely on its automated risk and event triggers (e.g., transaction monitoring systems). Where no risk triggers have been identified, there should be no need to actively update customer identification information, meaning that data correctness does not expire until there are reasons to doubt the correctness of client data and information. Once the customer has been identified, they remain identified (even if the passport’s validity expires), except in cases like a name change. Paragraph 2 of this Article would need to support this reading, in that if the monitoring process is effective, it would flag any relevant events, eliminating the need for additional outreach to customers. Specifically, under c): we ask for clarification of what would be considered “unexpected transactions”.

In **Article 22(2) of the RTS** “Customer identification data updates in low-risk situations” and recital (16), it is stated that “Obliged entities shall take the measures necessary to ensure that they hold up-to-date customer identification data at all times, and that they update the information they hold on customers onboarded before this Regulation within 5 years after the application date of this Regulation”.

Implementing this requirement in practice would create a significant administrative burden, as it would necessitate setting individual reminders for each ID document. This is particularly disproportionate in the context of Simplified Due Diligence (SDD), where due diligence files often contain multiple ID documents relating to different individuals - for example, in business relationships involving legal entities, joint accounts, or authorised representatives.

As a result, the same SDD relationship might have to be reviewed multiple times within a five-year period, undermining the very rationale of SDD. This approach risks creating negative consequences for clients, banks, and society at large.

Retail banking clients are frequently low-risk, and non-responsiveness to information requests may stem from factors such as limited awareness of financial crime issues, privacy concerns, or difficulties in obtaining supporting documents - particularly for vulnerable groups. Strict enforcement of relationship termination in such cases could lead to financial exclusion. Data should be retrieved in a way that is the less burdensome for society.

We encourage the EBA to consider a more proportionate approach that combines event-triggered and time-based updates. Specifically, for customers assessed as low risk, updates should be permitted via automated systems without the need to contact the customer. It should be clarified that banks may confirm or update customer information through automated processes that do not require operator or customer involvement.

Finally, we ask the EBA to confirm that the requirement to “hold up-to-date customer identification at all times” refers to situations where an obliged entity must conduct ongoing due diligence - either due to a time-based review or a relevant trigger event, such as a change in the customer’s name or gender. Routine refreshing of ID documents without a specific justification would unnecessarily increase operational costs and negatively affect the customer experience.

Regarding **Article 29 (1) a) iii**: Aliases and trade name: this implies that obliged entities are obliged to have this data in scope from targeted sanctions perspective. However, this information is not mandatory KYC information. There is a need for clarification on this.

## SIMPLIFIED DUE DILIGENCE FOR ULTIMATE BENEFICIAL OWNERS

### Article 19, Draft RTS – Minimum Requirements for the identification and verification of the beneficial owner or senior managing officials in low-risk situations

Regarding Article 19 of the Draft RTS, we understand this to mean that where the obliged entity holds official data from a reliable register such as a chamber of commerce or central UBO-registry, a simple confirmation by the customer of this information is sufficient. We support this interpretation and seek confirmation of this understanding.

Article 19 of the Draft RTS on the minimum requirements for the identification and verification of the BO or SMO in low-risk situations provides that, in low-risk situations, the obligated entity may consult one of the following sources for identification of the BO or senior management and use other sources from the same list referred to in point b) or c):

a. Information entered in the central register or in the commercial register;

b. The statement or explanation provided by the customer, including confirmation that the data is adequate, accurate and up to date for the purpose of verifying the identity of the beneficial owner or senior management;

c. Any source of public and reliable information, including internet research.

However, we would request clarification on the difference between “lower risk situations” as referenced in Article 18 and “low risk situations” as referenced in the title of Article 19. Further, we would like to gain a better understanding of

how both relate to the terminology used in Article 33 AMLR, which refers to a “low degree of risk”. We believe it is important that terminology across regulatory instruments is consistently aligned or clearly distinguished.

### Article 22, Draft RTS – Customer identification data updates in low-risk situations

On Article 22, we interpret this to mean that in low-risk situations – i.e., where there are no indicators of high risk – the obliged entity may rely on its automated risk and event triggers (e.g., transaction monitoring systems). Where no risk triggers have been identified, there should be no need to actively update customer identification information, meaning that data correctness does not expire until there are reasons to doubt the correctness of client data and information.

### Article 23, Draft RTS – Minimum information to identify the purpose and intended nature of the business relationship or occasional transaction in low-risk situations

In general, we notice that the articles in Section 4 are stricter than the AMLR, i.e. for source of funds and purpose and intended nature. In low(er) risk situations, the purpose and intended nature of the business relationship should primarily be derived from the type of product or service the customer obtains from the obliged entity. Art. 33 (1) lit c AMLR clearly allows this as a second option next to reducing the amount of information to be collected (“…OR inferring it from the type of transaction or business relationship established.”). Art. 23, Draft RTS does not reflect this option at all. We therefore request the EBA to explicitly clarify that Art. 23, Draft RTS does not exclude this second option – such an approach would once again go beyond the AMLR provisions. There is also no basis to require source of funds information by default. We once again would like to point out that the AMLR only requires obliged entities to collect information on the source of fund in the context of identifying the purpose and intended nature of a business relationship/occasional transaction where it is necessary to do so (see Art. 25 AMLR). This means the AMLR allows discretion and a risk-based approach in relation to the question which kind of information obliged entities shall collect to comply with the requirements prescribed in Art. 25 AMLR). This includes the decision not to collect any information on the source of funds if not considered to be relevant. Any other approach / interpretation would also undermine the principle of proportionality and the concept of SDD.

## ONGOING DUE DILIGENCE FOR ULTIMATE BENFICIAL OWNERS

### Article 24, Draft RTS – Additional information on the customer and the beneficial owners

We interpret the reference to “or the ownership and control structure” as applying only when relevant, and we seek clarification on what constitutes “verification of authenticity”. What are the minimum expectations regarding sources or documentation? We request clarification of what concrete additional

activities are expected for the verification of the authenticity and accuracy of the information on the customer and the beneficial owner.

**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 daft RTS? Please explain your rationale and provide evidence.**

As a general remark, we highlight the severe impact the provisions of Article 20 and Article 21 would have on correspondent banking and asset management services. Although the provisions in question are aimed at simplifying the CDD process, in reality they impose new, far-reaching requirements which entail a large and disproportionate increase in compliance costs for EU obliged entities.

**Article 20 of the RTS**

Section 4 of the draft RTS (Article 20) appears to bring pooled account arrangements within the scope of Article 20(1)(h) of the AMLR by allowing the application of simplified measures to fulfil the obligations outlined therein. Furthermore, the provision implies that, where the conditions listed in let. “a”-“d” are not met, identification and verification measures apply with regard to all natural persons that are customers of the customer of the credit institution, regardless of the amount of funds they have deposited in the account[1].We emphasise that, in practice, pooled accounts are typically opened by a financial institution for another financial institution in the context of a correspondent banking relationship (in majority of cases cross-border). The pooled account would consist of funds belonging to numerous underlying customers, whose number could be in the hundreds or even higher. Identifying and verifying the identity of each natural person behind the pool account would therefore result in a disproportionate amount of costs and compliance burden.

This is exacerbated by the fact that, in practice, the conditions listed in Article 20, let. “a”-“d” would rarely be cumulatively met, if ever. The most striking example is the condition under let. “c” whereby the ML/TF risk associated with the business relationship needs to be low. However, Article 36 of the AMLR requires specific EDD measures for cross-border correspondent relationships. Additionally, in its guidance for the securities sector, FATF has explicitly singled out pooled/omnibus accounts as running a high inherent risk for money laundering/terrorist financing[2]. Further difficulties arise in assessing AML/CFT requirements and effective AML/CFT supervision in third countries given the absence of an EU list of equivalent jurisdictions.

To address these concerns, we recommend the following:

- **Risk Classification**: Pooled accounts should not be presumed to be low risk. This would ensure alignment with both international market practice and the correspondent banking framework.
- **Broader Applicability**: The requirement under Article 20(1)(h) AMLR should be deemed fulfilled where the institution offering the pooled or omnibus account (not limited to credit institutions) has assessed the customer’s AML/CFT controls (as per letter (d) and with respect to the requirements laid down in Article 36 of the AMLR).
- **CDD Information Availability**: The institution should also be satisfied that the customer maintaining the pooled account will provide, upon

request, full CDD information and supporting documentation on its underlying clients.

Alternatively, a definition of the term “pooled account” may be included in the RTS, which would distinguish between cases involving correspondent banking relationships and other cases where the risks could indeed be lower, such as collective rent deposit accounts, escrow accounts of bailiffs and debt collection agencies, etc.

**Article 21 of the RTS**

Similarly to Article 20, Article 21 is a significant departure from the current approach applicable to asset management when a financial intermediary (asset manager) has entered into a business relationship with a collective investment undertaking involving both the fund and its investment manager.

Under the RTS, due diligence on final clients may be waived by the intermediary only if conditions identical to those in Article 20 have been met. If not, asset managers can no longer rely on due diligence performed by distributors. As described in the case of Article 20, the condition under Article 21, let. “c” is particularly problematic given that, if rated other than low, then the overall relationship could be out of the scope of SDD i.e. the Asset Manager would not be able to rely on the due diligence performed by the distributor in accordance with existing supervisory expectations. This would lead to an enormous and unmanageable impacts, potentially also negatively impacting retail investor participation.

Based on the above, we reiterate our proposals in relation to the provision of Article 20 to apply *mutatis mutandis* to Article 21.

---

[1] For example, according to the provision, where the SDD conditions are not met, a credit institution would have to identify and verify the identity of natural persons that hold even less than 1% of the funds in the pooled account.

[2] FATF – ‘Risk Based Approach Guidance for the Securities Sector’, October 2018, para. 82. Available at Risk-based Approach Guidance for the Securities Sector.

**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?**

We are particularly concerned that several EDD provisions impose overly rigid requirements. As noted in earlier comments, we recommend incorporating clearer references to the risk-based approach to allow obliged entities to tailor EDD measures to actual risk exposure. EDD is only meaningful when it is targeted to mitigate specific risks. In certain cases, existing information already held by banks may be sufficient to meet EDD requirements. This observation applies to all EDD-related articles discussed below.

**Article 24 of the RTS – Additional information on the customer and the beneficial owners**

We note that the wording “at least” in Article 24 introduces what appears to be a mandatory minimum list of additional information to be obtained by obliged entities. This appears to conflict with Article 34(4) AMLR, which states that EDD measures shall be proportionate to the higher risks identified.

The phrasing in Article 24, specifically “shall, at least” and the use of “and/or”, is ambiguous. It is unclear whether obliged entities are required to obtain all the information listed under subparagraphs **(a) to (d)**, or any one of them. To resolve this conflict and improve clarity, we recommend replacing “at least” with “where necessary”, thereby aligning the article with the proportionality principle in Article 34 AMLR.

**(a)** We interpret the reference to “or the ownership and control structure” as applying only when relevant, and we seek clarification on what constitutes “verification of authenticity”. What are the minimum expectations regarding sources or documentation? We request clarification of what concrete additional activities are expected for the verification of the authenticity and accuracy of the information on the customer and the beneficial owner.

**(b)** We welcome the explicit recognition of adverse media screening as an EDD-measure. This affirms our current approach and supports proportional application. It should be noted that reputational risk and ML/TF risks are distinct. We suggest seeking clarification to ensure that those factors that are considered relevant are the adverse media which are financial crime relevant.

**(c)** We interpret the reference to past business activities to be applicable only when risk-relevant, and request clarification on the expected time horizon for such assessments, to avoid unnecessary data collection. Point c) relatedly raises questions regarding the methods for collecting and documenting the beneficial owner’s previous business activities, as well as whether any changes should be tracked. Additionally, it is unclear how far back the documentation should cover. In our view a maximum of five years should not be exceeded, given that this is the maximum retention period stipulated by the EU AML regulation. A shorter period (e.g. three years) should be also sufficient.

**(d)** We wish to raise serious concerns regarding the expectation that obliged entities (OEs) collect information on family members, persons known to be close associates, and other close business partners or associates of the customer or beneficial owner (BO), in order to obtain a “holistic view” of ML/TF risks.

- **Risk of Tipping-Off and Jurisdictional Overreach -** While a comprehensive understanding of a customer’s risk profile is important, we caution that requesting such information - particularly in the context of potential suspicious activity - could in some cases amount to a tipping-off risk, especially where a Suspicious Activity Report (SAR) may be under consideration. Furthermore, investigating private associates and close relations may cross into the remit of law enforcement, going beyond the responsibilities and legal authority of obliged entities under AML/CFT compliance frameworks.
- **Proportionality and Link to Criminal Activity –** If, notwithstanding the questionable legality of requesting such information, the EBA decided to maintain the requirement of gathering information on associates or family members, then it should be clearly proportionate and based on an identifiable risk or potential link to criminal activity. Absent such a justification, such measures may be excessive, intrusive, and operationally unfeasible.

- **Data Protection and Privacy Concerns** - Point (d) also raises significant data protection concerns. Family members, close associates, and business partners are third parties with no direct relationship with the OE. Collecting and processing personal data about such individuals - often not publicly available - requires close scrutiny from internal data protection officers and may not comply with data protection principles. Under Article 76(2) of the AMLR, OEs may only process personal data if customers are adequately informed. It is unclear how this requirement can be fulfilled in the case of third parties who are unaware of the processing and who have no opportunity to consent or object.
- **Inconsistency with AMLR Articles 28 and 34** - We believe Article 24(d) goes beyond the intended scope of Article 28(1) AMLR, which governs enhanced due diligence (EDD), and is inconsistent with Article 34(4) AMLR, which limits the collection of additional information to that pertaining to the customer or beneficial owner. While extending due diligence to family members and close associates is appropriate and feasible for Politically Exposed Persons (PEPs) - given the public nature of their roles and the availability of relevant information - it is not practicable to apply this logic more broadly to all EDD cases.
- **Operational Impact and Legal Uncertainty** - Applying this requirement to every EDD scenario would result in substantial administrative burden, without clear parameters as to which relationships or individuals should be prioritised. This lack of specificity creates uncertainty as to the extent of due diligence expected. For non-PEP individuals with no public exposure, researching their personal and professional networks would be extremely time-consuming, often fruitless, and potentially legally questionable.
-

**Recommendation for Clarification and Limitation -** We therefore recommend that further clarification be provided on the specific circumstances under which information on family members, close associates, and business partners should be collected under Article 24(d). Such requirements should be clearly limited to cases where there is a demonstrable risk or suspicion, and where the individuals in question are reasonably identifiable and relevant to the risk assessment. Furthermore, the scope of such investigations must remain proportionate and consistent with data protection obligations under Article 76 AMLR.

**Article 25 of the RTS – Additional information on the intended nature of the business relationship**

Regarding a), the requirement for obliged entities to verify the legitimacy of the destination of funds raises questions about feasibility and scope. Specifically, it is unclear what “information from authorities” entails. Does this imply that obliged entities are expected to contact domestic or foreign tax authorities or FIUs as well as other obliged institutions[entities?] to verify where the funds are going? Such an expectation would be disproportionate, operationally impractical, and potentially conflict with data protection laws and the risk-based approach.

We suggest limiting this to publicly available information from (national) authorities.

Moreover, the clause reads “may include”, meaning that other sources are also possible. Henceforth it would be helpful to have an indication what the EBA had in mind here.

On b), we wish to clarification of what is expected when obliged entities are asked to verify the legitimacy of the expected number, size, volume, and frequency of transactions. If this implies substantiating each transaction with invoices, agreements, tax statements, or receipts for daily expenses such as food or utilities, it would be an extremely burdensome and unrealistic requirement for both customers and institutions. We consider that this, if required, such verification must be targeted at risk mitigation, rather than documentation for technical compliance purposes.

Moreover, it should be clarified whether such additional measures shall be undertaken only during the life of the relationship or also at the onboarding stage.

With regard to point (c), we question how the requirements set out in Article 25 align with the existing obligations under Articles 15 and 16 concerning the purpose and intended nature of the business relationship. There appears to be a significant overlap, and further clarification would help ensure consistent and proportionate application of these provisions.

**Article 26 of the RTS – Additional information on the source of funds, and source of wealth of the customer and of the beneficial owners**

Article 26(1) of the RTS lists the documentary evidence that may be accepted for proof of SoF and SoW in EDD business relationships. Unlike Article 24 and Article 25, does not allow evidence according to the assessment of the obliged entity. There is no apparent reason for this distinction and in light of the risk-based approach, obliged entities should be able to use other documents that have been referred to in order to verify source of funds/source of wealth.

As far as we understand there is no grandfathering-rule for business relationships that have been with the OE for a long time and have been established at a time where requirements like this have not been in place and as a result respective documentation has not been kept or has never been issued to start with.

Based on the requirements of Article 26 of the RTS, CDD could not be performed on such business relationships to the extend required and the OE would either have to pay fines for the violation or more likely try exit the customer, which will not be possible, as any other OE in the EEA will have the same requirements. Such customers would then be pushed out of the reach of the EU-AML legislation and retreat to destination with less stringent rules, which is certainly not a desired outcome. Henceforth a grandfathering rule should be implemented for business-relationships of a certain age.

The requirement to verify that the source of funds or source of wealth is derived from lawful activities using one or more forms of evidence sets an extremely high bar even as an EDD measure. This appears to reflect expectations more appropriate for forensic auditors or law enforcement investigations rather than for obliged entities conducting CDD in accordance with a risk-based approach.

(a) The expectation that pay slips or employment documentation must be signed by the employer is outdated and incompatible with modern digital payroll systems, where physical signatures are not the norm.

(b) The requirement to obtain certified copies of audited accounts appears unnecessarily burdensome, particularly when the same information is publicly available through official registers. Where accounts have already been audited by a recognised audit firm, the auditor's signature should be sufficient proof of authenticity - additional certification adds little value and should not be required.

More broadly, for all references to "certified copies", the RTS should clarify who is authorised to perform such certification. In particular, if an obliged entity has reviewed the original document, it should be permitted to retain a copy and certify that it has seen the original, without the need for certification by an external party.

(d) For assets stemming from inheritance, the availability of public official documentation cannot be assumed. In many jurisdictions, inheritance may be settled informally within families where the legal heir is obvious and no will exists. Such cases should be accommodated with alternative forms of evidence or declarations.

(g) It would be appropriate to provide an example of the type of documentation expected (e.g. documents issued by government bodies?) or of the independent or reliable sources to be considered for this purpose.

**Article 27 of the Draft RTS – Additional information on the reasons for the intended or performed transactions and their consistency with the business relationship**

Point a) requests the verification of the accuracy of the information on legitimacy of the intended outcome of an intended or performed transaction. It is unclear how an OE should verify if the funds are genuinely being used as intended and announced to the OE. This obliges OEs to investigate on a level that is 1) not legitimate for an OEs as these are tasks allocated to FIUs and law enforcement; and 2) will involve third parties that the OE has no access to.

In relation to b), we request further clarification on how "consistency" is to be determined and what criteria are to be used to evaluate whether transactions align with the customer's business activities and turnover. Should we understand "assets representing higher risks" to refer to business activities where there are large price fluctuations, high-value low-volume assets, or high-value transactions?

With reference to c), the obligation to assess the legitimacy of the parties involved in a transaction, including intermediaries and their relationship to the customer, appears to imply a requirement to conduct CDD on the customer's business partners. This is neither feasible nor appropriate for obliged entities and should not form part of the EDD requirements.

Furthermore, where the counterparty is a customer of another financial institution, especially when located in the EEA, obliged entities should be permitted to rely on the presumption that the counterparty's bank has fulfilled its own CDD obligations in line with EEA regulations.

We propose that even in high-risk situations requiring EDD, if a transaction clearly falls within the expected transaction profile of the customer and is consistent with the nature of the business relationship, it should not trigger an obligation to conduct additional scrutiny. EDD should be focused on deviations from expected behaviour.

Proposed alternative wording for Article 27:

*Additional information or assessment on the reasons for the intended or performed transactions and their consistency with the business relationship.*

*The additional information obliged entities obtain on the reasons for the intended or performed transactions and their consistency with the business relationship, in accordance with Article 34(4), point (d) of Regulation (EU) 2024/1624 shall enable the obliged entity to:*

*a. Determine the transaction activity and whether this activity is consistent with the expected behaviour for this customer or category of customers*

*b. Determine whether transactions that are assessed by the obliged entity to be complex or unusually large follow a suspicious pattern without any apparent economic or lawful purpose.*

**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?**
**Comment on Screening Obligations under Article 29 of the Draft RTS**

Article 29 of the Draft RTS requires obliged entities to screen “at least...the date of birth”. We note, however, that date of birth has not traditionally been used as a standalone screening criterion. Screening is, for good reason, almost exclusively based on the name of the relevant party.

While the date of birth can support the validation of alerts triggered by name-based screening, it is neither appropriate nor necessary as a primary screening field. Dates of birth are significantly less unique than names of parties, which would result in a higher volume of false positives. These false hits, often completely unrelated to the sanctioned party, would require manual dispositioning and create an undue operational burden.

Moreover, sanctions target individuals, not abstract data points. Legal designations are based on names, not dates of birth. Names - combined with fuzzy logic matching techniques - are sufficient to generate meaningful alerts, which can then be refined using additional identifiers, such as date of birth or address, where available in the sanctions list information.

Requiring screening against date of birth is therefore disproportionate, inefficient, and misaligned with established practice.

**Request for Alignment with Existing Guidance on Targeted Financial Sanctions**

The area of Targeted Financial Sanctions is already governed by its own established guidelines and best practices. To avoid inconsistencies (and potential conflicts), we request that the relevant articles are aligned with both the Council of the European Union’s Best Practices for the Effective Implementation of Restrictive Measures (“EU Best Practices”) and the EBA Guidelines on

internal policies, procedures, and controls for the implementation of Union and national restrictive measures under Regulation (EU) 2023/1113 (EBA/GL/2024/15).

We note, however, that Section 4.1.4, paragraph 17 of EBA/GL/2024/15 currently includes an incorrect reference to date of birth as a screening field - an issue already highlighted in our preceding comments on date of birth. This reference should be rectified to ensure consistency and accuracy in implementation.

**Clarification on Scope of (Targeted) Screening under Article 28 of the Draft RTS**

The current wording in Article 28 of the Draft RTS - “all entities or persons which own or control such customers” - could be interpreted as requiring obliged entities to screen all intermediary ownership layers between the customer and the Ultimate Beneficial Owner (UBO).

We believe that screening should be focused on the customer and those individuals or entities that ultimately own or control the customer. Including the term “ultimately” ensures clarity and aligns the obligation with the principle of identifying persons with meaningful ownership or control, thereby avoiding unnecessary and disproportionate screening.

We therefore propose the following revised wording for Article 28 of the Draft RTS:

“To comply with Article 20(1)(d) of Regulation (EU) 2024/1624, obliged entities shall apply screening measures to their customers and to all the entities or persons which ultimately own or control such customers.”

**Request for Terminological Consistency in Draft RTS**

We note that Article 29 lit. (a) of the Draft RTS requires, in the case of a natural person, screening of the name “in the original and/or transliteration of such data”. At the same time, Recital 3 refers to the collection of data “in the same way in relation to the transcription of...” for identification and verification purposes.

To ensure clarity and consistent application, we request alignment and clarification of the terminology used - particularly with respect to *transliteration*, *transcription*, and related requirements.

Similarly, we note inconsistent use of the terms *trade name*, *commercial name*, and *registered name* across the draft RTS (e.g. in Articles 1, 18, and 29). We recommend harmonising these terms to avoid ambiguity and ensure uniform interpretation.

**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?**
NA

**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?**
**Article 32 of the RTS**

We interpret Article 32 of the RTS on CDD as introducing a five-year period within which all customer identification information must be updated for existing customers, in accordance with Article 22(1) of these RTS. In our view, customer identification data includes all CDD elements, such as the identification of the customer (name and date of birth), ownership and control structure, UBO, SMO, and legal representatives. This reading is consistent with recital 16 of the RTS and recital 43 of the broader EBA consultation document.

Although Article 32 refers to the entry into force of the RTS, we consider that the five-year period is intended to begin from the application date of Regulation (EU) 2024/1624 (the AMLR), as confirmed in Article 90 of the AMLR, which sets this date as 10 July 2027. Recital 16 of the RTS supports this interpretation by explicitly referring to the “application date” as the moment from which the update obligation should be calculated. Accordingly, we interpret Article 32 to mean that all existing customer information must be updated, in a risk-based manner, by no later than 10 July 2032.

In line with recital 43, we will prioritise customer files that present a higher risk. The order in which banks will review and update lower risk customers will be based on the banks’ internal risk assessments and ensuring compliance within the five-year timeframe.

In addition, banks will treat event-driven reviews - such as alerts, unusual transactions, or other relevant risk indicators - as a trigger to update the customer identification information, irrespective of the originally planned periodic review cycle.

Finally, while the obligation to update information formally applies from 10 July 2027, we are of the opinion that banks may begin updating identification data before that date where operationally feasible, and do not have the obligation to have that finished already by 2027” (in accordance with the EBF call for a grace period). Given that the AMLR has already entered into force, we have concluded that early updates are supported by a legitimate interest under the GDPR and will enable operational readiness.

**Question 1: Do you any have comments or suggestions regarding the proposed list of indicators to classify the level of gravity of breaches sets out in Article 1 of the draft RTS? If so, please explain your reasoning.**
NA

**Question 2: Do you have any comments or suggestions on the proposed**

**classification of the level of gravity of breaches sets out in Article 2 of the draft RTS? If so, please explain your reasoning.**
NA

**Question 3: Do you have any comments or suggestions regarding the proposed list of criteria to be taken into account when setting up the level of pecuniary sanctions of Article 4 of the draft RTS? If so, please explain your reasoning.**
NA

**Question 4: Do you have any comments or suggestions of addition regarding what needs to be taken into account as regards the financial strength of the legal or natural person held responsible (Article 4(5) and Article 4(6) of the draft RTS)? If so, please explain.**
NA

**5a: restrict or limit the business, operations or network of institutions comprising the obliged entity, or to require the divestment of activities as referred to in Article 56 (2) (e) of Directive (EU) 2024/1640?**
NA

**5b: withdrawal or suspension of an authorisation as referred to in Article 56 (2) (f) of Directive (EU) 2024/1640?**
NA

**5c: require changes in governance structure as referred to in Article 56 (2) (g) of Directive (EU) 2024/1640?**
NA

**Question 6: Which of these indicators and criteria could apply also to the non-financial sector? Which ones should not apply? Please explain your reasoning.**
NA

**Question 7: Do you think that the indicators and criteria set out in the draft RTS should be more detailed as regards the naturals persons that are not themselves obliged entities and in particular as regards the senior management as defined in AMLR? If so, please provide your suggestions.**
NA

**Question 8: Do you think that the draft RTS should be more granular and develop more specific rules on factors and on the calculation of the**

**amount of the periodic penalty payments and if yes, which factors should be included into the EU legislation and why?**
NA

**Question 9: Do you think that the draft RTS should create a more harmonised set of administrative rules for the imposition of periodic penalty payments, and if yes, which provisions of administrative rules would you prefer to be included into EU legislation compared to national legislation and why?**
NA

**Name of the organization**
European Banking Federation (EBF)