RTS under Article 40(2) of the AMLD

Question 1: Do you have any comments on the approach proposed by the EBA to assess and classify the risk profile of obliged entities?

The Association answer:

We would like EBA to clarify and advise on certain items:

1. **Definition and Standardisation of Methodologies**

Can the EBA confirm whether the methodology for determining inherent and residual risk, including the scoring system and weightings of indicators, will be defined at EU level either by EBA or AMLA, rather than left to national supervisors? For example, RTS mentions pre-determined thresholds multiple times (e.g., Articles 2(1), 3(1)), stating that numerical scores should be assigned based on pre-determined thresholds. However, it does not define what these thresholds are, who sets them, or how they are determined. A unified, centrally defined approach is essential to ensure comparability, reduce regulatory arbitrage, and avoid divergent applications of risk assessment methodologies across Member States. Delegating this responsibility to national supervisors may lead to fragmented implementation and diverging supervisory practices.

2. **Clarification of Proportionality Principle**

Can the EBA clarify how the principle of proportionality will be operationalised in practice within the RTS, and whether further guidance or formulaic thresholds will be provided in other RTS? The current draft refers to proportionality but lacks a concrete framework or examples. RTS does not provide a formula or detailed explanation for how this proportionality is calculated. The term "proportional" is used qualitatively, not mathematically.

3. **Clarification and Expansion on "Major Events"**

Can the EBA expand the definition of "major events" and provide more detailed guidance or a non-exhaustive list of events that would trigger supervisory review or risk reclassification? At present, the term is too vague. More clarity is needed to ensure that all supervisors apply consistent criteria when considering events such as cyber breaches, changes in ownership, mergers, or shifts in business models. The RTS should prevent divergent interpretations in similar scenarios.

4. **Sector-Specific Considerations**

Will the EBA or AMLA develop sector-specific annexes, reference documentation, or indicator modules to reflect the diverse risk profiles and control environments of different types of obliged entities (e.g., CASPs, EMIs, banks, crypto platforms)? A modular approach would ensure that indicators are relevant and proportionate to the entity type, improving accuracy and supervisory outcomes. A uniform set of indicators may fail to account for sector-specific risk drivers.

5. **Remittance Transfer Thresholds in Product/Service Risk Assessment**

Could clarification be provided on why, under the Products and Services assessment, remittance transfers above 1,000 EUR are included, while lower-value transfers are excluded? In practice, lower-value transfers are more likely to be conducted anonymously and may carry higher ML/TF risk, while transfers above 1,000 EUR typically involve verified customers and established relationships. The current inclusion criterion appears counterintuitive and would benefit from further rationale or adjustment.

6. **Request for Exemption for Low-Risk, Narrow-Scope Entities**

Would the EBA consider introducing an explicit exemption from the reporting and assessment obligations under Articles 2 and 3 for entities whose activities are strictly limited in scope and demonstrably low-risk? We propose the following exemption clause be added to both articles:

"By way of derogation from this Article, the obligations laid down herein shall not apply to institutions that provide only payment initiation services and/or are engaged solely in the collection of payments for utilities or other regularly provided services intended to meet household needs, the collection of fines and/or other levies for state authorities, or the disbursement of social benefits."

Proportionality and risk-based approach: Entities falling within the above description are characterised by a limited service offering, low complexity, and minimal exposure to ML/TF risks. Applying complex risk-scoring obligations in such cases would be disproportionate.

Operational burden vs. supervisory value: These requirements may impose significant administrative costs while offering limited added value to supervisors.

Consistency with EU AMLD objectives: This proposal is aligned with Directive (EU) 2024/1640, which advocates a risk-based and proportionate supervisory regime.

We trust this request will be taken into consideration in the interest of maintaining a proportionate and risk-sensitive reporting and supervisory framework.

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.

The Association answer:

We support the EBA's proposal whereby the residual risk score of an obliged entity cannot exceed its inherent risk score.

Question 3: Do you have any comments on the proposed list of data points in Annex I to this Consultation Paper? Specifically,

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?

The Association answer:

Currently, essential client information is extracted automatically from identity documents, such as passports or national IDs, through digital onboarding channels and vendor-supported verification tools. These systems are configured to parse standard, widely-available fields such as name, date of birth, nationality, and document number. However, place or country of birth is not always present, structured, or required in standard identity documents across jurisdictions. As such, requiring these fields would necessitate systemic changes at multiple levels of the onboarding and compliance infrastructure.

In the short term, financial institutions would incur direct vendor costs to gain access to additional data fields and verification capabilities, where available. At the same time, institutions would need to redevelop existing API integrations and user interfaces on client-facing channels to accommodate these new requirements. This demands scarce engineering and development resources and introduces delays in deployment pipelines, particularly where onboarding platforms are integrated with third-party services and internal systems (e.g. CRMs, screening engines, or risk scoring tools).

In the medium term, maintaining and scaling these solutions imposes ongoing operational and technical costs. Data collection workflows would need to be redesigned to capture and store new fields, often with manual fallback mechanisms in cases where source documents do not provide the required information. Compliance teams would need to update internal policies, adjust screening algorithms, and provide staff training on how to verify, input, and assess new types of data. Institutions would also be responsible for ensuring data quality, consistency, and protection under applicable data privacy regimes, including GDPR, which creates further risk and liability exposure.

The long-term impact is particularly severe for existing customer populations. Retrospective data collection of place or country of birth would require large-scale data remediation projects, which are resource-intensive and often disruptive. These projects involve contacting clients, verifying additional information manually or through alternative means, and managing exceptions. In large institutions, such efforts can span multiple business units and jurisdictions, creating complex governance challenges and diverting capacity away from core risk-based AML/CFT work.

Moreover, each new data point introduces cascading dependencies across multiple compliance, technology, and operational layers. This amplifies the cost not just financially, but also in terms of implementation risk, customer friction, and regulatory exposure. For digital-first or cross-border institutions, the challenge is even greater, as onboarding flows must accommodate jurisdictional variations in available data and regulatory interpretations.

We respectfully suggest that new mandatory data fields should be required only where there is a clear, risk-based justification, and where such fields are reliably available from standard, authoritative sources (e.g. identity documents). In line with the principle of proportionality and Regulation (EU) 2024/1624's risk-based approach, we propose that institutions should have the flexibility to collect such data points where relevant and appropriate, rather than as an absolute minimum requirement across all customer types and scenarios.

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?

The Association answer:

Before addressing individual data points, we would like to highlight a broader concern regarding the structure and consistency of the indicators listed in Annex I. The wording and structure of the data fields vary significantly across different categories and subcategories, including across product lines (e.g. payment accounts vs. lending). In some cases, data is requested in terms of the number of customers, in others the value of transactions, and occasionally both. Additionally, some indicators are quantitative, while others are qualitative, sometimes expressed as a percentage without clear context or methodology.

This lack of consistency raises the question of whether the differences are intentional or accidental. If intentional, it would be helpful for EBA to clarify the rationale behind requesting different types of data for different product lines or services. It is also unclear why only certain products require qualitative data (e.g. percentage-based inputs), while others do not. A more uniform structure, for example, requesting either the number of customers or the total value of activity across all relevant indicators, would significantly improve clarity and reduce the implementation burden on institutions.

Moreover, many of the data points are challenging to evaluate in the absence of technical specifications, calculation formulas, or predefined reporting formats. Without access to the detailed reporting instructions or templates that will eventually accompany these RTS, it is difficult to assess the feasibility and accuracy of data collection, particularly where data is not readily available in current systems.

Section A and Customers data group:

1. **Number of legal entities with a complex structure:** This data point is currently not available in a standardised format. While a draft RTS on customer due diligence (CDD) introduces a definition of "complex structures", the document has not yet been adopted and remains subject to change. Institutions currently apply varying internal definitions of complexity (e.g., based on ownership layers, offshore elements, or nominee structures), and there is no consistent classification across the market. If the RTS definition changes before adoption, financial institutions (FRDs) will be required to revisit historical data and reclassify existing customers, which may require significant resources. In light of this, we suggest considering the temporary removal or deferral of this data field until the RTS is finalised.

2. **Number of customers registered abroad by country (legal entities):** This data is partially available; however, the term “abroad” lacks clarity. It is not specified whether it refers to entities registered outside the EU, outside the institution’s home country, or outside the licensing jurisdiction. Institutions require a consistent definition to ensure comparability and proper mapping. We recommend that this term be clarified in future iterations.

3. **Number of walk-in customers:** This data point is ambiguous and not currently tracked in most systems. If the term “walk-in” is intended to refer to physical, branch-based customer interactions, this may only apply to institutions with physical presence and might not reflect risk accurately. If it is meant to describe occasional or non-recurring customers, this should be clearly stated. We suggest replacing this with the legally defined term “occasional transactions” and aligning it with terminology under AMLD/AMLR.

4. **Number of occasional transactions carried out by walk-in customers:** This indicator combines transactional and customer-specific data, and should logically fall under the “Products, Services and

Transactions" category. Furthermore, as noted above, without a clear and standardised definition of "walk-in customer," this data cannot be extracted reliably from existing systems.

5. **Number of customers with high-risk activities:** This data point is highly subjective and is not available in a reliable or standardised format. For legal entities, activity-based risk scoring (e.g., based on sectoral codes or typologies) may exist, but for natural persons, this information is rarely collected or classified. Additionally, "high-risk activity" is defined differently across institutions depending on their internal risk methodology, national risk assessments, and supranational guidance. The lack of harmonisation means that the data will not be representative and could mislead supervisory assessments. A single institution's customer base might appear disproportionately high- or low-risk due to internal methodology, not actual exposure.

6. **Number of customers with FIU requests linked to AML/CFT matters:** This data is not available. Financial Intelligence Unit (FIU) or law enforcement requests typically do not specify the nature of the investigation. As such, institutions are unable to reliably determine whether a request relates to AML/CFT concerns specifically (as opposed to fraud, cybercrime, or tax matters). Tracking this information would require assumptions and subjective categorisation, which undermines consistency and data reliability.

Section A and Products, Services and Transactions data group

1. **Correspondent services:** Additional explanation is necessary to determine what types of relationships or services fall within this definition. Under currently proposed wording, "correspondent services" could encompass a wide range of inter-institutional arrangements, including general business relationships between financial institutions. A more precise and operationally clear definition would help prevent inconsistent interpretation across the market.

2. **Factoring:** This service is currently presented as a separate data group from "Trade Finance." However, factoring is often regarded as a subcategory of trade finance. For clarity and alignment, it would be helpful either to integrate factoring under the "Trade Finance" heading or to provide a justification for treating it separately. Additionally, a clear definition of "Trade Finance" is needed.

Section A and Distribution Channels data group

Number of new customers onboarded in the previous year by third parties not directly subject to AML/CFT supervision: This data point appears to relate to reliance-based onboarding models; however, the phrase "not directly subject to AML/CFT supervision" lacks sufficient clarity. It is uncertain whether this refers to entities outside the EU framework, non-regulated introducers, or third parties relying on group-wide policies. To ensure consistent interpretation and implementation across Member States, a more precise definition is needed. We would recommend further clarification on the types of entities considered "not directly subject" and whether their status is to be assessed based on jurisdictional supervision or internal risk-based criteria.

Section B and 2B. Customer ML/TF Risk Assessment and Classification (CRA) data group

Number of customers per ML/TF risk category (low risk, medium-low risk, medium-high risk, high-risk): The inclusion of four specific risk levels effectively introduces an implicit standardised risk categorisation.

However, obliged entities may apply different classification models tailored to their risk appetite, business model, or jurisdictional requirements – ranging from three to more than four categories. To accommodate this diversity, we suggest either removing the enumerated risk levels from the brackets or clearly stating that they are indicative examples rather than mandatory categories.

Section B and 3A. Customer Due Diligence data group

Several data points in this section would benefit from clarification, particularly regarding their scope and intended interpretation:

Number of customers for whom no information has been obtained on the nature of the customers' business, or of their employment or occupation (excluding customers with whom the obliged entity does not have a business relationship)

Number of customers (excluding natural persons) for whom beneficial ownership identification details are entered in the institution's database

Number of customers, who are natural persons, for whom all identification details (name / date of birth, nationality, tax number) are entered in the institution's database

In our view, these indicators seem to be designed to identify gaps in customer data. However, as currently worded, it is not entirely clear whether they are intended to report on cases where the relevant information is missing or where it is present. We would welcome confirmation from the EBA regarding the correct interpretation. If the aim is to flag instances where information has not been obtained or recorded, the language should be adjusted accordingly to prevent misinterpretation and ensure consistent reporting across institutions.

Section B and 3C. Transaction Monitoring

The framing of one of the follow-up questions in this section raises conceptual concerns. While it is acknowledged that institutions are increasingly relying on artificial intelligence and machine learning technologies to detect suspicious activity, the question as formulated appears to shift the supervisory focus toward verifying consistency between transaction data and pre-recorded CDD information. This narrows the purpose of transaction monitoring to a form of static data validation, rather than supporting its broader and more dynamic function, namely, identifying unusual or unexpected patterns of client behaviour that may indicate money laundering or terrorist financing risks.

"If automated system: The system can generate alerts in case of inconsistencies between CDD information relating to the customer and the following elements: a) Number of transactions b) Value of aggregated transactions c) Value of single transactions d) Counterparties e) Countries"

We suggest reconsidering the scope and formulation of this indicator. The current approach may not reflect the operational reality or the evolving capabilities of transaction monitoring systems. A more risk-based and outcome-focused formulation could better align with supervisory expectations and market practices. Additionally, clarification is needed as to whether this item is intended to assess the functionality of automated systems or to quantify actual instances of mismatches between CDD data and transaction patterns.

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

The Association answer:

No particular comments.

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.

The Association answer:

We remain supportive of the EBA's overall objective to harmonise supervisory methodologies and enhance ML/TF risk oversight. However, we believe that careful calibration of implementation timelines, audit requirements, and frequency thresholds is critical to achieving these goals in a proportionate and sustainable manner.

We respectfully submit that the current **deadline of nine (9) months** for supervisors to carry out the first assessment and classification of inherent and residual risk profiles under Articles 2, 3, and 4 of this Regulation, as set out in Article 5, **is insufficient given the complexity, breadth, and technical implications of the required data and systems.**

1. Insufficient timeline for initial implementation

In particular, we would like to highlight the following critical concerns:

1. Regulatory uncertainty and incomplete definitions since key risk indicators such as "complex structures" are not yet formally defined. The draft RTS on CDD, where such definitions are expected, has not been adopted, and there remains a real possibility of change. Without finalised definitions, obliged entities and supervisors alike cannot reliably classify or report this information. Premature application of such requirements risks legal uncertainty and inconsistent interpretation across Member States.

2. The scope of Annex I, particularly Section A, includes numerous data points that are not currently collected or maintained in structured formats. Many institutions will need to develop or adapt classification criteria, implement new data taxonomies, and reconfigure internal systems to meet the requirements. Even for technically advanced institutions, this represents a significant operational and IT undertaking that cannot reasonably be completed within a 9-month window.

3. Supervisors themselves will require time to design and deploy tools, scoring models, and review protocols to carry out consistent risk classification. These changes also require training and capacity building across supervisory teams.

In light of the above, we propose extending the initial implementation deadline in Article 5 from nine (9) months to fifteen (15) months following the entry into force of the Regulation. This would ensure alignment with the timeline for adoption of the relevant RTS and accompanying guidelines, allow both supervisors and obliged entities to apply the Regulation with legal certainty, safeguard proportionality,

especially for smaller firms, and promote a level playing field and prevent implementation shortcuts that could compromise data quality and risk assessment reliability.

2. Clarification on supervisory use of audits

We would also like to raise questions about the expected frequency of supervisory assessments and the possible reliance on audits in support of annual reviews.

The text suggests that AML audits may be expected annually to support the yearly classification of risk profiles. Currently, in jurisdictions such as Lithuania, such audits are required once every two years, which represents a well-balanced and proportionate approach. Moving to annual audits would result in a substantial increase in compliance costs, with estimates ranging upwards of EUR 50,000 per audit. This level of cost would be disproportionate for smaller firms and may be unsustainable for much of the market. We recommend that annual supervisory risk assessments should rely primarily on existing data (e.g. Enterprise-Wide Risk Assessments, monitoring outputs, and periodic internal reviews), and external audits should remain biennial unless specific concerns arise.

Additionally, we note that the RTS refers repeatedly to "external auditors" in the context of supervisory assessments (e.g., Article 3(3b), Section 4.2). It is unclear why emphasis is placed on external audit when many institutions maintain robust and independent internal audit functions. Internal auditors often provide higher-frequency oversight, possess deep system knowledge, and contribute directly to governance through continuous monitoring and remediation.

Therefore, the RTS should not imply that only external auditors are acceptable for AML/CFT assessments. We suggest revising the language to state that "an appropriately qualified and independent auditor or specialist" may conduct assessments, with independence ensured by separation from the function under review. This approach preserves the value of internal audit, while maintaining supervisory integrity.

Furthermore, we seek clarification regarding the statement in Article 3(3) that supervisors may collect data "from the obliged entities or external auditors… or other bodies." It is unclear whether this introduces a new power for supervisors to directly obtain data from external auditors without going through the obliged entity itself. This raises concerns regarding the legal basis for such access, potential supervisory overreach, and practical implementation challenges.

If no such direct access power is intended, we strongly recommend that the RTS be revised to avoid ambiguity. Specifically, the reference to "external auditors" should be reconsidered, or alternatively, "other bodies" should be clarified as "other competent authorities or institutional bodies" to maintain legal clarity and avoid unintended consequences.

3. Cost differences between normal and reduced frequency

The difference in compliance burden between the two options (normal (annual) and reduced (triennial) reviews) is significant, particularly for institutions with limited resources. Annual reviews imply not only greater data collection, validation, and reporting effort, but also recurring internal or external audit engagements, additional resource allocation, and system strain. For institutions eligible for reduced frequency, the ability to spread assessments over three years would yield substantial savings. These include

lower audit or assurance-related costs (potentially up to EUR 50,000 per cycle), reduced strain on compliance staff, extended timeframes to implement corrective actions, system improvements, or data enhancements.

We strongly support the introduction of reduced frequency for low-risk institutions, as outlined in the draft RTS. This tiered approach will help maintain proportionality, preserve resource efficiency, and foster a risk-based supervisory culture.

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.

The Association answer:

No particular comments.

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.

The Association answer:

We submit that cross-border transactions involving jurisdictions within the EEA should be assessed differently from those involving third countries when determining geographical risk exposure. There are several compelling reasons for this:

1. EEA countries are bound by common AML/CFT legislation, including Regulation (EU) 2024/1624 and related directives, which ensure harmonised minimum standards, risk-based supervision, and consistent implementation across the Union. Financial institutions operating within the EEA are subject to equivalent rules and oversight mechanisms, reducing jurisdictional uncertainty.

2. The EU single market is underpinned by the principles of mutual trust and regulatory equivalence. Financial institutions operating on a cross-border basis within the EEA benefit from passporting rights, allowing them to provide services in other Member States without duplicative authorisation or assessment procedures. Treating EEA cross-border flows as equivalent to those with third countries would undermine this legal construct and create unnecessary friction in the internal market.

3. Applying the same level of scrutiny to intra-EEA transactions as to third-country relationships would not reflect the actual risk profile, which is mitigated by the shared legislative, supervisory, and enforcement environment in the EEA. Such an approach would be disproportionate, leading to inflated risk assessments and unwarranted operational burdens, particularly for smaller or cross-border institutions.

4. Institutions would be forced to apply duplicative controls to EEA-based relationships, despite those jurisdictions being subject to the same AML/CFT rules. This misallocation of resources could dilute focus on genuinely higher-risk jurisdictions outside the EU/EEA framework.

We therefore recommend that geographic risk assessments should clearly distinguish between transactions involving EEA jurisdictions and those involving third countries. Risk classification should only elevate

intra-EEA relationships where there is reliable evidence of jurisdiction-specific deficiencies or systemic ML/TF threats not based solely on cross-border status.

RTS under article 12(7) AMLAR

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.

The Association answer:

We appreciate the EBA's efforts to introduce materiality thresholds to help calibrate supervisory attention to cross-border activities carried out under the freedom to provide services. However, we would like to raise concerns regarding the ambiguity in the current drafting of Article 1(1) and Article 1(2). In particular, we request clarification on **whether the thresholds are intended to apply cumulatively (i.e. both must be met).**

Specifically:

Article 1(1)(a) sets a threshold of 20,000 customers resident in a given Member State.

Article 1(1)(b) refers to a threshold of EUR 50 million in incoming and outgoing transactions generated by the customers referred to under letter (a).

These points are connected **by the conjunction "or,"** which typically suggests alternative (disjunctive) criteria.

However, the cross-reference in point (b) to the customers "referred to under letter (a)" strongly implies that the EUR 50 million threshold only applies where the 20,000-customer threshold is already met, indicating that both criteria must be fulfilled for materiality to arise. This would also imply that the EUR 50 million threshold must be met in each Member State where services are provided, consistent with Article 12(1) of Regulation (EU) 2024/1620, which requires assessments in at least six Member States. **This interpretation clearly points to a cumulative application of the thresholds.**

In contrast, Article 1(2) states that materiality is met "where the activity … meets any of the materiality thresholds referred to in paragraph 1 points (a) and (b)," which suggests a disjunctive reading—i.e. that either threshold may be sufficient on its own. This inconsistency creates legal uncertainty and could lead to diverging interpretations by market participants and supervisors.

We therefore respectfully recommend that the EBA **explicitly clarify that the thresholds in Article 1(1)(a) and (b) are intended to apply cumulatively**. We consider this approach to be both proportionate and consistent with the apparent drafting intent and the structure of Article 12 of Regulation (EU) 2024/1620.

Additionally, in the interest of adhering to a risk-based approach, we recommend refining the customer count criterion by **considering only active customers**, that is, those who have carried out at least one transaction in the past year. This would more accurately reflect the actual scale and risk profile of cross-

border operations, particularly in business models where a relatively small number of clients may generate substantial transaction volumes (e.g. B2B services).

Data on active customers is already expected to be collected under Annex I, Section B, making this refinement both practical and impactful. It would also help avoid disproportionate outcomes where dormant or legacy accounts inflate customer counts without contributing to risk exposure.

We believe these adjustments would support a more coherent and risk-aligned application of the materiality test across the Single Market.

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.

The Association answer:

At this stage, we believe it would be premature to consider lowering the thresholds in Article 1 before clarifying how they are intended to operate. As noted in our response to Question 1, the current drafting leaves room for interpretation, particularly around whether the thresholds apply cumulatively or disjunctively.

Clear guidance on this point would provide a more solid basis for assessing whether the threshold levels are proportionate. Assuming a cumulative application (i.e. both criteria must be met), the current thresholds seem appropriate and balanced, targeting genuinely material cross-border activity without creating undue burden on smaller or specialised firms.

We would therefore recommend prioritising clarification of the existing text before revisiting the threshold values. Once the wider regulatory framework is more settled, it will be easier to assess the long-term impact and determine whether any adjustment is needed.

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.

The Association answer:

We recommend reconsidering the use of a single customer threshold irrespective of customer type, as it may not accurately reflect the nature or scale of AML/CFT risks.

Legal entities, particularly in sectors such as crypto, gambling, or complex cross-border services, typically carry higher inherent AML/CFT risks than retail clients. A firm serving a small number of institutional or high-risk business clients may pose significantly greater risk than one serving a larger retail base, yet may fall outside the scope of materiality under the current 20,000-customer threshold.

Applying a uniform threshold may thus lead to disproportionate outcomes, undercapturing high-risk business models while placing undue focus on lower-risk retail operations that happen to exceed the numerical threshold.

We would therefore support a differentiated approach, whereby separate thresholds are established for retail and institutional clients. This would allow supervisors to better capture material activity in line with the underlying risk, and improve proportionality in supervision. For example, a lower numerical threshold could be applied to legal entities, reflecting their generally higher risk profile, while retaining a higher threshold for natural persons.

Such differentiation would also align with broader risk-based principles in AML/CFT regulation and support more targeted and effective supervision across diverse business models.

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.

The Association answer:

No particular comments.

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.

The Association answer:

No particular comments.

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 Association answer:

No particular comments.

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 Association answer:

No particular comments.

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?

The Association answer:

No particular comments.

Question 9: Do you agree with the transitional rules set out in Article 6 of this RTS? In case you don't, please provide the rationale for it and provide evidence of the impact the EBA's proposal and your proposal would have.

The Association answer:

No particular comments.

RTS under Article 28(1) AMLR

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?

The Association answer:

While we strongly support the overarching objective of harmonising and strengthening customer identity verification across the EU, we respectfully do not fully support the proposals as currently set out in Section 1 of the draft RTS. Several obligations introduce new requirements that are not clearly supported by the Level 1 Regulation (EU) 2024/1624 and risk conflicting with core AML/CFT principles such as legal certainty, proportionality, and the risk-based approach. In particular, the provisions related to both customer identity and beneficial ownership verification appear to exceed the legal mandate, constrain the application of risk-based assessments, and impose disproportionate administrative and operational burdens, especially for low-risk scenarios and cross-border arrangements. Furthermore, the prescriptive nature of the draft RTS restricts the use of digital onboarding innovations and automated processes, which are essential for maintaining efficiency and accessibility in modern compliance frameworks. This could lead to reduced effectiveness without delivering commensurate improvements in AML/CFT outcomes. ***To address the above concerns, we recommend the following adjustments to the draft RTS:***

1. **Article 1, we propose the following revision**: "*Obliged entities shall obtain at least those names that feature on the customer's identity document, passport or equivalent.*" This formulation maintains the necessary flexibility for fully digital or registry-based onboarding processes and avoids imposing unnecessary manual interactions in low-risk or automated environments. It ensures alignment with the risk-based approach while supporting innovation in the Fintech sector.

2. **Article 1(3), we propose removing the reference to** "*commercial name*", restoring alignment with the Level 1 text and avoiding unnecessary operational burden to mitigate below listed concerns and preserve the effectiveness of the AML/CFT framework. Alternatively, EBA should provide a clear definition of "commercial name" (e.g., how it differs from trademarks or informal trading styles), specify it must be obtained only if it is formally registered in the business register or clarify whether verification of the commercial name shall not be required and such information may be collected based on self-declaration by the customer. This would allow entities to apply the requirement consistently and proportionately.

3. **Article 3**, **we would suggest the provision on the customer's place of birth should preferably read:** "*...shall consist of the country na*me." or, alternatively, "*...shall consist of both the city and country name, where such information is available on official documents.*" This adjustment would ensure that the requirement reflects the actual content of commonly used ID documents, avoids imposing unrealistic verification obligations, and reduces the risk of onboarding errors due to inconsistent data availability or formatting.

4. **Article 4**, **we recommend the following wording:** "*...shall obtain information on the nationality of the customer, as established through reliable documentation. Where justified by risk, obliged entities shall*

assess whether additional nationalities may exist and take proportionate steps." or, alternatively, *"...shall obtain information on the customer's nationality through official documents or self-declaration, and assess the need to investigate further based on risk-based considerations.*" These options recognise the practical limitations of verifying multiple nationalities and ensure proportionality by linking additional investigative steps to concrete risk factors.

5. The draft RTS currently lacks sufficient guidance on the manner and scope of data collection for legal representatives, as required under Article 22(1)(b)(iii) of the AMLR. Notably, the Level 1 text specifies that only the name of the legal representative must be collected. In this context, **we seek clarification on the following two points**:

5.1. Interpretation of "*legal representative*": Whether this term is to be interpreted in accordance with national civil, corporate, or administrative law frameworks (e.g., powers of attorney, statutory representatives, or board-authorised officials); and

5.2. Exhaustiveness of data collection obligation: Whether the requirement to collect only the name is to be interpreted as exhaustive, thereby excluding the need to collect other personal data points (such as nationality, date or place of birth), which are otherwise required for natural persons under the RTS.

Addressing these questions is essential to ensure legal certainty and operational consistency across Member States. Legal representation frameworks vary significantly between jurisdictions, and overextending data collection requirements without clear legal basis could create inconsistency, increase compliance burdens, and lead to inefficiencies, particularly for entities handling a large volume of legal person customers.

6. **Article 5 should explicitly recognize national documents if they are currently considered as such by the separate countries**. In other words, RTS should explain that any identity document or equivalent issued by a Member State that is valid for identification under national law is acceptable for Regulation Article 22 purposes even if it lacks one or more fields listed in Article 5(1) by confirming that where certain data points (e.g., city of birth, biometric data) are missing from valid ID documents, obliged entities may proceed based on the assessed risk without needing to escalate or reject the document. Also in this context the definition of "*Legitimate Reasons*" should be defined in RTS Article 5(2) to ensure consistent interpretation.

7. **The RTS should recognise internal linguistic capacity where appropriate, as well as the use of trusted translation tools.** It should also clearly state that certified translations are not required by default but only where risk and context justify such a measure. Furthermore, we urge inclusion of clear criteria for who qualifies as a certifier to avoid divergent interpretations.

8. **EBA should confirm that certified copies are only required in exceptional cases and not as a default expectation by adjusting the Article 5(4) language to**: "*Where appropriate, a copy may be accepted based on a risk-based assessment by the obliged entity.*" Also if the definition of "*certified copy*" remains used, RTS should provide a definition and clarify who is authorised to issue it.

9. **Article 7 should provide further guidance on how obliged entities are expected to operationalise the requirement to assess whether an information source is** "*reliable and independent.*" Specifically: (i)

Is this assessment required for all information sources used during customer identification (e.g., public registries, commercial databases, identity documents), or only for third-party electronic sources used to supplement identity verification? (ii) Is it sufficient to apply internal procedural controls and retain evidence supporting such evaluation as part of general CDD procedures (e.g., maintaining a list of sources deemed reliable and independent)? (iii) Is this assessment also required when identity verification is based solely on the customer's official identity document (passport, ID card, etc.), particularly where such documents already undergo formal issuance processes with embedded security features as described in Article 6 of the RTS?

10. **EBA should confirm and clarify that customer-provided information may be used directly under the RTS Article 9 where appropriate within the institution's risk-based framework.** Clarify that data obtained directly from customers may constitute a "reasonable measure" under Article 22(7)(b), especially for low-risk relationships or when corroborated by other sources.

11. **We would encourage EBA to also explicitly recognise registry aggregators and technical intermediaries (e.g., providers of automated access to official registers) as reliable sources under Article 9(a)**, provided they apply appropriate integrity safeguards since this supports digitalisation, reduces administrative burden and aligns with the EU digital agenda.

12. **RTS should define or provide EU-level guidance on** *"independent professional"* **used in RTS Article 9(b)** to avoid inconsistent national interpretations. Clarify whether this includes regulated professionals, notaries, or internal compliance officers.

13. **EBA should clarify** *"reference to the existence of any nominee shareholder"* **under Article 10(1)(b) since the term is unclear and difficult to apply in jurisdictions where nominee arrangements are contractual and not publicly disclosed**. We propose defining the term or linking it to formal registration obligations i.e., references to nominee shareholders should be based on official disclosures or public corporate registries. Alternatively, clarify what level of documentation or self-declaration is acceptable.

14. **EBA should also clarify the scope of information required under Article 10(1)(c). The requirement to collect information on the "**regulated market**" where securities are listed (Article 10(1)(c)) lacks clarity.** It is not specified whether this refers solely to the name/jurisdiction of the exchange, or if additional details (e.g., securities held, extent of listing) must be collected. So, we suggest EBA specify the level of detail required under Article 10(1)(c), for example, confirming whether it is sufficient to collect the name and jurisdiction of the listing exchange, or whether deeper analysis is expected.

13. **It is highly suggested to treat "multi-layered" criterion as one of several indicators, not a determinant under Article 11(1)**. "Multi-layered" ownership should be treated as a potential indicator of complexity, prompting further risk-based inquiry not as an automatic trigger for classifying a structure as complex when combined with other factors. This would better align with the principle of proportionality in the AMLR. Also we would think that a rigid threshold, such as defining two layers of ownership as inherently complex, would undermine the risk-based approach. Instead, the assessment should focus on whether the structure lacks a legitimate economic rationale or impairs identification of the beneficial owner. Alternatively, structural complexity could be defined as involving four or more layers, but only where such

a configuration obstructs transparency or traceability. This would align with Article 11(2), which calls for ownership charts to clarify such structures.

14. **We would also suggest considering removing or rewording Article 11(1)(d) to eliminate the vague reference to** "non-transparent ownership with no legitimate economic rationale." If retained, the language should be narrowed to "*structures that lack legitimate economic rationale and obscure the beneficial ownership or ownership chain.*"

1. Lack of Legal Basis in Level 1 Text

First, there is a lack of legal basis in the Level 1 Text since several obligations go beyond the mandate granted by Article 22 of Regulation (EU) 2024/1624 and thus risk exceeding the scope of Level 2 technical standards, undermining legal certainty and potentially exposing obliged entities to disproportionate compliance risks:

1. **Customer Names (Article 1):** The requirement to "ask the customer to provide" their names, which implies direct customer involvement not expressly required by the Level 1 text. This restricts the flexibility afforded by digital or automated onboarding processes, especially where identification is based on qualified electronic signatures or verified eID systems. This formulation imposes a method of interaction rather than focusing on the outcome (obtaining verified names), which is not mandated at Level 1.

2. **Commercial Name of Legal Entities (Article 1(3)):** The requirement to collect and verify a legal entity's commercial name (or "doing business as" name) has no explicit basis in Level 1 text, which only requires obtaining identifying information of the legal person. Introducing this obligation risks legal uncertainty and may conflict with the principle that RTS must remain within the Level 1 framework.

3. **Place of Birth (Article 3):** The draft RTS mandates collection of both the city and country of birth, imposes a granular data requirement not stipulated in the Level 1 text. The inclusion of "city" lacks clear legal grounding and is not necessary to meet the core objective of identifying the customer. Making "city" mandatory creates a new Level 2 obligation, absent from Level 1, and risks violating the principle of legal certainty.

4. **Nationalities (Article 4):** The obligation to "satisfy themselves that they know of any other nationalities" extends the interpretation of Article 22(1)(a)(iii), which only requires obtaining information on "nationalities...where applicable". This formulation implies a duty of investigation or verification that is not foreseen in the Level 1 text, and risks setting an unreasonable standard for due diligence. Also the use of the term "satisfy themselves" is vague and not sufficiently legally sound, thus it would suggest using clearer alternatives.

5. **Documents for the verification of the identity (Article 5):** Article 22 of Regulation (EU) 2024/1624 sets the foundation for customer identification but does not require the inclusion of specific data fields such as biometric data, machine-readable zones, or signatures. However, the draft RTS expands the identity verification requirements beyond what is explicitly mandated at Level 1 by requiring that documents include fields such as city of birth, biometric data, and a machine-readable zone; introducing certified copy and certified translation obligations without an express mandate from Level 1; applying rigid document format criteria that diverge from accepted national identity practices. These additions create legal

uncertainty and risk conflicting with the principle of legal clarity. For example, many national identity documents or driving licences are valid for identification under national laws but may not meet all the prescriptive criteria of Article 5(1). Therefore, RTS should align strictly with the provisions of Article 22 and refrain from introducing additional substantive requirements (e.g., biometric data, signature), and documents should be considered acceptable if they are valid for identification purposes in the issuing Member State. Additionally, we note a typographical error in the draft RTS Article 5(4): the reference to Article 22(6)(a) is currently incomplete, with the letter "a" missing. We respectfully request that this be corrected for legal clarity and consistency.

6. **Beneficial Ownership Verification (Articles 9 and 10):** Article 22(7)(b) of AMLR explicitly allows verification of the beneficial owner through "reasonable measures" which may include "*obtaining information, documents and data from the customer or other reliable sources.*" This dual-source approach reflects the intent to maintain flexibility and proportionality, enabling entities to tailor verification methods according to the risk and context of the relationship. However, Article 9 of the RTS appears to deviate from this by omitting the customer as a permissible direct source, unless the data is "*certified by an independent professional.*" This is not only inconsistent with the AMLR's wording but implicitly redefines what is considered a "*reasonable measure,*" without a clear legal basis. Moreover, the RTS uses a mandatory phrase "*shall obtain the following information,*" but it is unclear whether this obligation aligns with AMLR Article 22(7)(b), which permits the use of "*reasonable measures*" to obtain data from "t*he customer or other reliable sources.*" This creates potential confusion around whether information obtained directly from the customer, especially in low-risk or straightforward cases, would satisfy the obligation, and what level of verification (e.g., documentation) is required for each data point.

7. Furthermore, the **RTS introduces the undefined concept of** "*independent professional,*" which lacks a harmonised EU definition, causing legal uncertainty, especially in cross-border contexts where national interpretations vary. It is unclear whether this includes in-house compliance staff, regulated professionals (e.g., lawyers, notaries), or other categories. This ambiguity poses serious practical concerns, particularly in cross-border contexts where national interpretations of professional qualifications and obligations vary significantly. Institutions may be unsure whether information certified by an in-house compliance officer, a regulated lawyer abroad, or a corporate service provider would satisfy the RTS requirement. This ambiguity could result in divergent practices and challenges in implementation.

8. Additionally, Article 20(1)(b) of the AMLR generally requires obliged entities to understand the ownership and control structure of their customers but does not define thresholds or prescribe automatic triggers for assessing whether a structure is "*complex.*" The AMLR also does not define "*multi-layered*" ownership. However, the RTS introduces a prescriptive criterion by defining "***multi-layered*" as involving two ownership layers and treats this as a determinant factor for structural complexity**. There is no clear legal basis for classifying a structure as complex solely on this basis, especially where transparency is intact, a legitimate economic rationale exists, and no ML/TF red flags are present.

We recommend raising a clarification regarding the definition of a "*complex ownership structure.*" It is unclear why the current definition considers a structure with two layers across different jurisdictions as complex. In practice, structures with two layers typically allow for clear and straightforward identification of ultimate beneficial owners. Therefore, we suggest revising the definition to reflect a higher threshold,

such as four or more ownership layers combined with involvement of multiple jurisdictions, which would more accurately represent genuinely complex ownership arrangements.

2. Risk-Based Approach Limitations

Secondly, Section 1 appears to introduce significant limitations on the application of the risk-based approach, which is a fundamental principle underpinning AML/CFT frameworks. The draft RTS sets out uniform, prescriptive customer identification requirements that apply irrespective of the customer's risk profile, onboarding context, or the nature of the business relationship. This undermines the principle that AML/CFT measures must be proportionate to the level and type of risk.

1. **Customer Name Collection (Article 1):** The obligation to "*ask the customer*" for specific name elements limits the use of digital identity solutions and hampers innovation. This approach is particularly problematic for low-risk or fully verified digital onboarding processes, where entities should retain flexibility to apply streamlined measures. By enforcing a rigid requirement regardless of risk, the draft discourages low-risk digital onboarding models, models which are actively encouraged under EU digital finance initiatives as part of broader goals to enhance financial inclusion and technological development.

2. **Commercial Name Collection (Article 1(3))**: From a risk perspective, the commercial name of a legal entity offers limited AML/CFT value. Obliged entities already verify the customer's legal name, registration number, beneficial ownership, and controlling structure, factors that are far more relevant for understanding and managing ML/TF risk. In contrast, commercial names are often used purely for branding or marketing purposes and may not correspond to the entity's legal or risk identity. Furthermore, the line between a commercial name and a trademark is often unclear, as trademarks are governed by intellectual property law and may belong to a different legal entity altogether. Requiring the inclusion of commercial names in customer due diligence (CDD) checks may lead to confusion or misalignment between branding and legal identity, without improving AML/CFT outcomes. As with the other elements noted above, applying this requirement uniformly without consideration of its actual risk relevance contradicts the principles of proportionality and effectiveness that define a risk-based approach.

3. **City of Birth Collection (Article 3):** The mandatory collection of a customer's city of birth does not provide material value for mitigating money laundering or terrorist financing risks, particularly when the country of birth and current residential address are already obtained. Identity documents across the EEA and globally vary in whether they include city of birth, leading to inconsistency and potential onboarding issues. Discrepancies may arise when different documents show different spellings or formats of the same city (e.g., a passport versus a residence permit), which may appear as mismatches in CDD checks. In many cases, firms may be compelled to request birth certificate documents not typically accepted as sole proof of identity to verify this information, thereby complicating compliance unnecessarily. Moreover, the city of birth does not typically inform jurisdictional risk assessments and does not materially enhance the differentiation of customer profiles from an AML/CFT perspective.

4. **Verification of All Nationalities (Article 4)**: Imposing a blanket requirement to identify and verify all nationalities of a customer is misaligned with risk-based standards. While some jurisdictions (e.g., Lithuania) may include this as a national requirement, most EEA countries including Sweden, Malta, and Belgium recognize dual or multiple citizenships without routinely verifying all of them during CDD.

Official identity documents typically only confirm the nationality of the issuing country, and there is no unified EEA or global database that enables verification of other nationalities. In practice, it may be impossible to identify or confirm second or third nationalities, particularly if acquired after the issuance of a primary ID document. Such a requirement should be limited to cases where contextual risk factors exist such as ties to high-risk jurisdictions, PEP status, conflicting documentation, or possible sanctions exposure. Without such indicators, enforcing this obligation universally imposes significant operational burden without a corresponding benefit to risk mitigation.

5. **Documents for the verification of the identity (Article 5)**: Under this Article, draft RTS applies uniform and prescriptive requirements that are not commensurate with the varying risk levels of different customer types or onboarding scenarios. In particular, nationality and place of birth including city, even some observations above would be relevant here but additionally we want to note that requiring all these elements in all cases disregards the fact that many national documents include only the country of birth, but not the city some of them may omit nationality (e.g. drivers licenses even issued EU, some examples Austria https://www.consilium.europa.eu/prado/en/AUT-FO-05002/image-240431.html; Belgium https://www.consilium.europa.eu/prado/en/BEL-FO-05001/image-320546.html; or Lithuania https://www.consilium.europa.eu/prado/en/prado-documents/LTU/F/docs-per-category.html). Collecting this data in all cases provides little risk mitigation in low-risk situations. Also worth mentioning that biometric data and signature and other technical features that are not data points in their sense are unavailable in certain instances, e.g. especially for minors, non-residents, or when onboarding is conducted remotely and certain earlier issued identity documents that may still be valid and acceptable under certain national laws of Member States (some examples: residence permits in Austria: https://www.consilium.europa.eu/prado/en/AUT-HO-14002/index.html; Belgium: https://www.consilium.europa.eu/prado/en/BEL-HO-29001/index.html etc.). The RTS should explicitly permit flexibility to adjust identity verification requirements based on the customer's risk profile. Additional data (e.g., biometric features, city of birth) or document formats (e.g., certified copies) should only be required when the risk-based assessment supports their necessity.

6. **The same RTS Article 5 also introduces additional format requirements for other types of documents i.e. certified translations and certified copies.** Firstly, the draft implies a broad obligation for certified translations, although Article 5(3) allows discretion "*when deemed necessary.*" This phrase, however, lacks definition and invites inconsistent application. Then, Article 5(4) implies a general requirement for certified copies. This risks undermining digital identity verification, imposes high costs, and lacks grounding in Level 1. Furthermore, there is currently no harmonised EU standard that defines "*certified translation*" or "*certified copy.*" This ambiguity increases the risk of inconsistent interpretation and application across Member States. We recommend that the RTS provide clear guidance on what constitutes a certified copy, including who may issue it and the level of formality required.

7. **Limitations on the Risk-Based Approach (Articles 9 and 11):** The RTS, particularly in Article 9 and Article 11, introduces prescriptive requirements that may override the principle of proportionality and undermine the risk-based approach embedded in the AMLR. For instance, excluding the customer as a primary source in the absence of external certification, even in low-risk relationships, could lead to disproportionate compliance obligations. Additionally, Article 11 introduces automatic criteria for deeming

structures "*complex*" (e.g., two ownership layers or cross-jurisdictional registration), regardless of the actual ML/TF risk or transparency. This approach may result in unnecessary application of enhanced due diligence (EDD) for otherwise low-risk and transparent corporate structures, overreliance on form over substance in determining risk, potentially detracting from ML/TF mitigation effectiveness. Structures with two ownership layers, even spanning multiple jurisdictions, can be straightforward and pose minimal AML risk, especially when beneficial ownership is clearly identifiable. Automatically designating such structures as "complex" may trigger unwarranted EDD in low-risk scenarios, contrary to the risk-based approach. Additionally, criterion (d) under Article 11(1), "non-transparent ownership with no legitimate economic rationale" is particularly vague and risks leading to inconsistent or arbitrary interpretations by obliged entities and regulators.

The risk-based approach is a cornerstone of the AML framework, requiring obliged entities to apply measures proportionate to the nature and level of ML/TF risk. The current draft RTS, however, appears to favour a rigid, prescriptive model by restricting acceptable sources of beneficial ownership verification to a narrow list, sidelining the flexibility embedded in the AMLR. By effectively excluding the customer as a source unless additional certification is applied, the RTS may lead to over-implementation of controls in low-risk scenarios. Furthermore, the draft RTS does not adequately account for modern, risk-sensitive solutions provided by third-party registry aggregators, which offer indirect access to official data from multiple public registries across jurisdictions. These platforms often implement quality controls, real-time updates, and integrity checks that can exceed manual verification processes. Failing to explicitly recognize such intermediaries undermines technological neutrality and may hinder innovation in AML compliance.

3. Administrative Burden

Last but not the least there will be a disproportionate administrative burden for the Fintech sector. If adopted in its current form, Section 1 of the RTS could impose substantial operational, legal, and financial costs, particularly on small and mid-sized financial institutions, payments firms, and fintechs operating across multiple jurisdictions. Beyond increasing workload and compliance expenses, the RTS's prescriptive requirements pose significant constraints on the use and development of digital innovation and automated solutions in AML compliance. Examples include:

1. Extended onboarding times and customer friction due to mandatory certification requirements that cannot be fully met through automated digital processes alone.

2. Reconfiguration of KYC and onboarding workflows, including renegotiation of contracts with identity verification providers and legal reviews of third-party certifiers, undermining streamlined digital onboarding journeys and increasing manual intervention.

3. Duplication of effort, where institutions cannot rely on previous verification done by other credit or financial institutions, hindering the effectiveness of shared digital platforms and registry aggregator services.

4. Increased costs for both FIs and customers due to mandated use of third-party professionals for certification or documentation, which may discourage adoption of innovative, technology-driven identity verification methods.

5. Fragmented implementation across the EU, as national competent authorities interpret undefined terms and requirements differently, creating barriers to interoperable digital solutions and cross-border data exchange.

By excluding direct customer data and un-certified sources from acceptable verification methods, the RTS fails to adequately recognise the capabilities of modern, automated AML technologies such as real-time data integration from official registries, AI-driven risk scoring, and trusted digital identity verification platforms. This restriction significantly limits the use of scalable, technology-enabled AML processes, resulting in increased manual checks, longer processing times, and higher operational costs.

Small and mid-sized fintech firms, which often rely on cutting-edge digital tools to onboard customers efficiently and comply with AML requirements, may face disproportionate burdens. They will be forced to adopt costly manual processes or rely on external certifiers, undermining their competitive advantage and slowing innovation in the EU financial ecosystem. Examples from Section 1 includes but is not limited (also refer to comments already provided above):

1. **Customer Name Collection (Article 1):** The wording, which demands "*asking the customer*" for full names, may obstruct automated onboarding flows, such as those using eID or registry-based KYC, where the customer is not actively entering data. To comply, entities would have to redesign fully digital journeys and introduce unnecessary manual steps.

2. **Commercial Name Collection (Article 1(3)):** Introducing a mandatory requirement to collect and verify commercial names will cause additional operational strain, particularly for smaller or digital-only providers. In many EU Member States, commercial names are either not systematically registered or appear only in non-digitised, regional registries that are not publicly accessible. Sole traders and SMEs may operate under informal commercial names that are unregistered and unverifiable. These names often appear only in unstructured formats such as websites, invoices, or marketing materials none of which are reliable or standardized sources. To comply, institutions would need to rebuild onboarding systems to accommodate new data fields, design logic for validating informal or unverifiable names, retrain staff and potentially conduct customer outreach to obtain or clarify data. These efforts would come at a considerable cost, while offering minimal AML/CFT value, since commercial names do not reflect legal ownership or control. For Fintech firms operating with lean infrastructure and high automation, this requirement would result in disproportionate compliance obligations with limited regulatory return.

3. **City of Birth Collection (Article 3):** Many official ID documents (e.g. in Lithuania, Netherlands, Estonia, Sweden, Switzerland, USA) do not include this information, or include it in inconsistent formats. Collecting this data would require manual workarounds, free-text entry systems (increasing error rates), additional verification steps, and customer clarifications, all of which reduce efficiency and increase onboarding times. A few concrete examples: Lithuania, Estonia or Norway: passports show only country of birth https://www.consilium.europa.eu/prado/en/LTU-AO-04005/image-370778.html ; https://www.consilium.europa.eu/prado/en/EST-AO-06001/image-334615.html ; https://www.consilium.europa.eu/prado/en/NOR-AO-06001/image-333924.html ; Netherlands: passports do not list place of birth at all: https://www.consilium.europa.eu/prado/en/NLD-AO-05001/image-342202.html Sweden and Switzerland: fields refer to place of origin or mother's residence,

not actual city of birth: https://www.consilium.europa.eu/prado/en/CHE-AO-04001/image-361045.html ; https://www.consilium.europa.eu/prado/en/CHE-AO-04001/image-361045.html ; The United States may list only the state (e.g. Washington D.C.) or country of birth, while for individuals born abroad, only the country may appear. https://www.consilium.europa.eu/prado/en/USA-AO-04001/image-102526.html etc. Requiring this data would create disproportionate barriers for onboarding without any proven benefit to risk mitigation.

4. **Collection and Verification of All Nationalities (Article 4):** Identity documents generally show only the issuing country's nationality. In the absence of access to government registries or international citizenship databases, it is not feasible to verify additional nationalities independently. Imposing a universal obligation would require: system changes to collect and store this information; questionnaire design, escalation processes, and staff training; greater friction for legitimate customers, especially where the information is non-material or outdated. This would significantly increase operational cost with marginal, if any, gain in AML/CFT effectiveness.

5. **Documents for the verification of the identity (Article 5):** Operationalising the requirements set out in the draft RTS will generate significant compliance costs and operational complexity, without delivering proportional benefits in terms of risk mitigation. Systems will need to be adapted to capture and validate additional data fields; however, this will not eliminate the need for manual processing. Where documents do not contain specific fields, such as the city of birth, staff will be compelled to carry out manual reviews or request supplementary documents, introducing delays, increasing workloads, and reducing efficiency in the onboarding process. Certified translations, in particular, are costly, time-consuming to obtain, and impractical in the majority of onboarding scenarios. Moreover, the RTS does not define what constitutes a "certified translation," nor does it provide guidance on who qualifies as a certifier. This lack of clarity leads to inconsistencies and potential miscommunication between customers and obliged entities, who may struggle to explain not only what is required, but—more importantly, why these requirements exist. Similar concerns arise with the requirement for certified copies. Mandating such documents undermines digital onboarding frameworks, is often impractical—especially in cross-border or digital contexts—and does not necessarily improve the reliability of identity verification. In remote or rural areas, obtaining certified copies can be especially burdensome, potentially excluding otherwise legitimate customers from financial services. The costs associated with translations and certifications also introduce financial barriers, particularly for individuals, small and medium-sized enterprises (SMEs), and customers based in lower-income or high-friction jurisdictions. These burdens are difficult to justify in low-risk scenarios.

Therefore, the RTS should make clear that requirements for certified translations and certified copies are exceptions, applicable only in high-risk cases or where other, risk-based verification methods are unavailable or insufficient. In addition, the RTS should provide precise definitions for both "certified translation" and "certified copy," including who may issue them and the level of formality expected, in order to avoid divergent interpretations across Member States. Only such an approach can be considered forward-looking and aligned with broader EU initiatives aimed at modernisation, digitalisation, and financial inclusion in an increasingly globalised environment.

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.

The Association answer:

We appreciate the efforts to establish robust safeguards for remote customer verification under Article 6 of the draft RTS. However, we have significant concerns regarding legal coherence with the Level 1 text, the prescriptive nature of the current draft, and the potential operational burden it imposes. Our detailed comments are structured as follows:

1. Legal Interpretation of Article 6(1) and Technological Neutrality

We are concerned that Article 6(1) of the draft RTS risks departing from the legal intent and technological neutrality of the Level 1 text. The draft currently states: *"…obliged entities shall 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…".* While we understand and support the objective of promoting secure identification methods, the current drafting could be interpreted as elevating eIDAS-compliant solutions to a default or exclusive status for remote identification, thereby treating all other remote verification methods as exceptional. This interpretation lacks a clear basis in Article 22(6)(a) of the AMLR, which permits identification based on the submission of identity documents, potentially accompanied by information from reliable and independent sources, without prescribing a preference for eIDAS-based methods.

Such prioritisation of eIDAS undermines the risk-based, proportionate, and technologically neutral approach that underpins both the AMLR and broader EU digital regulatory frameworks. In practice, many obliged entities across Member States already employ robust remote verification methods, such as biometric authentication, video identification, and liveness detection, that are approved by national competent authorities and have demonstrated assurance levels equivalent to or greater than those under eIDAS. These methods are essential for maintaining secure, scalable, and user-friendly onboarding, particularly in jurisdictions where eIDAS-based solutions remain unavailable or impractical due to infrastructure or legal constraints.

Moreover, the current wording may create unnecessary legal ambiguity around the permissibility of using electronic identification means provided by non-qualified providers, even where these solutions meet the 'substantial' or 'high' assurance levels set out in Regulation (EU) No 910/2014. This would be contrary to the principle of technological neutrality and could severely limit the use of innovative and widely accepted digital identity tools.

To address this concern and ensure consistency with the AMLR's enabling provisions, we recommend amending the text of Article 6(1) to clearly allow for the use of electronic identification means that meet the appropriate assurance levels, regardless of whether they are provided by qualified trust service providers. This would confirm that both qualified and non-qualified solutions when offering the required levels of security are permissible.

2. Proportionality and Technological Neutrality in the Application of Article 6(2)

We are concerned that the draft RTS takes a prescriptive, one-size-fits-all approach to customer identification, which conflicts with the core principles of proportionality, risk sensitivity, and technological neutrality set out in the AMLR. By implicitly positioning eIDAS-compliant methods as the default or preferred approach, regardless of the actual risk level or technological context, the RTS may impose undue burdens on obliged entities and limit access for certain customer groups.

Implementation of eIDAS varies significantly across Member States, and in some jurisdictions, coverage remains limited or fragmented. Mandating the use of eIDAS-based identification as a primary means risks excluding or disadvantaging legitimate customers, including non-EU nationals (such as refugees, cross-border workers, or foreign students) who may not possess eIDAS credentials. This requirement also creates disproportionate compliance costs for digital-first institutions, such as FinTechs, microfinance providers, and neo-banks, who rely on streamlined remote onboarding flows that are secure, user-friendly, and scalable.

Furthermore, the draft text fails to recognise that many alternative identification methods, such as biometric facial recognition, sequential image capture with liveness detection, or trusted first-payment verification mechanisms, can achieve high assurance levels without resorting to complex and costly procedures like real-time encrypted video chats (as required under Article 6(4)(b)). These alternatives are already used effectively and securely across multiple EU markets, with strong auditability and proven fraud prevention results.

We do welcome the inclusion of fallback mechanisms in Article 6(2), which acknowledge that high-assurance eIDAS solutions or qualified trust services may not always be available. However, to fully align with the AMLR and safeguard cross-border service provision. The phrase "*or cannot reasonably be expected to be provided"* introduces legal ambiguity and could lead to disproportionate administrative burdens. Without clearer guidance, obliged entities might interpret this as requiring them to actively prove the unavailability of specific solutions through documented evidence, failed onboarding attempts, or even burdensome inquiries with customers. Such obligations would contradict the principles of technological neutrality and proportionality and risk chilling innovation and competition in the market. We therefore recommend clarifying that the determination of whether a solution "*cannot reasonably be expected to be provided*" should rest with the obliged entity, based on a risk-sensitive and context-specific assessment. In particular, the assessment should take into account the technological maturity, commercial feasibility, and market penetration of the identification method in question, the jurisdictional or regional availability of electronic identification means meeting the 'substantial' or 'high' assurance levels under Regulation (EU) No 910/2014, regardless of whether they are notified in the EU under that Regulation; and the operational capacity and established partnerships of the obliged entity, including whether the entity has access to trusted and secure identification providers.

These clarifications would preserve the necessary flexibility for obliged entities to tailor their onboarding flows to real-world conditions and customer needs, while maintaining strong safeguards against impersonation and identity fraud. They would also promote consistent implementation across Member

States, helping to avoid market fragmentation and support the freedom to provide services under the EU Single Market framework.

3. Administrative Burden

Moreover, it is unclear whether the requirement applies to personal identity documents or to business registration documents for legal persons; if the latter, this should be clearly stated. There is also ambiguity around the practical implications: does the presence of a security feature, such as a hologram, eliminate the need for additional verification (e.g., cross-checking registry information), or is it supplementary? This should be clarified.

Furthermore, key terms like "*original document," "reproduction,"* and "*security features*" are undefined, potentially leading to inconsistent implementation and over-compliance. We recommend clarifying whether "original document" includes digitally issued documents with qualified electronic signatures or seals, which are increasingly used across Member States and by corporate clients. The use of the term "reproduction", which is inconsistent with "copy" used elsewhere in the RTS, adds confusion and should be harmonised to avoid divergent interpretations.

It appears that the RTS refers explicitly to identity documents (such as an identity card, passport, or equivalent) only in the context of natural persons. By contrast, it does not specify which documents are appropriate for verifying the legal establishment of legal persons. The only explicit requirement is that information provided by legal persons must be verified through reliable and independent sources. This stands in contrast to the considerable emphasis placed on data collection and verification requirements for natural persons, while offering limited practical guidance on the verification of legal persons. Consequently, Article 6(5), which introduces specific obligations concerning document features (such as security elements), creates additional ambiguity by not clearly distinguishing whether these obligations apply to documents relating to natural or legal persons. Greater clarity and proportionality are needed to ensure that the RTS adequately addresses the operational realities of verifying legal persons, including the use of public registers, certified registry extracts, and company data obtained through authorised digital channels such as APIs.

Recommendations and Required Clarifications

To align the RTS with the Level 1 AMLR and uphold risk-based and innovation-friendly implementation, we respectfully recommend the following:

1. Amend Article 6(1) as follows:

"*To comply with the requirements of Article 22(6) of Regulation (EU) 2024/1624 in a remote identification context, obliged entities shall use:*

(a) electronic identification means which meet the requirements of Regulation (EU) No 910/2014 with regard to the assurance levels 'substantial' or 'high', whether or not provided by a qualified trust service provider; and/or

(b) relevant qualified trust services, as set out in that Regulation."

This clarification would uphold the flexibility intended by the Level 1 text, promote continued innovation in remote identification practices, and prevent fragmentation across Member States.

2. Clarify the application of Article 6(2), including the interpretation of "*cannot reasonably be expected to be provided*," and confirm the continued validity of alternative identification methods under Article 22(6)(a). Relevant factors may include the technological maturity, market penetration, and commercial feasibility of the solution, the jurisdictional or regional availability of electronic identification means that meet the 'substantial' or 'high' assurance levels under Regulation (EU) No 910/2014, regardless of notification status under that Regulation, and the operational capacity of the obliged entity, including access to trusted providers. At the same time, we recommend confirming that, where high-assurance eID means or qualified trust services are not available or cannot reasonably be expected to be provided, obliged entities may rely on secure and reliable processes aligned with Article 22(6)(a). These include the submission and verification of identity documents (e.g., passports, national IDs), supported by measures such as biometric liveness detection, trusted metadata check etc. Such practices are already widely used across the EU and should not be relegated to exceptional cases. Preserving this flexibility is essential to ensure proportionality, uphold technological neutrality, and allow for a risk-based approach to Customer identification.

3. Reframe Article 6(4)(b) to focus on outcomes (e.g., secure identity and presence verification) rather than prescribing a specific communication medium. Permit other methods that offer equivalent or superior assurance (e.g., biometric liveness detection, trusted digital signatures, secure metadata checks) to support technological neutrality and equivalence.

4. Define key terms such as "*original document," "reproduction,*" and "*security features*" to ensure legal clarity. Confirm whether official electronic documents (e.g., digitally issued extracts) qualify as "*originals.*" Also, if the term "reproduction" is used in the final RTS text in the same context, clarify whether it refers to captured images of natural persons' ID documents used during remote onboarding, or applies exclusively to documents representing legal persons (e.g., articles of incorporation, registry extracts). Confirm that digitally issued or certified documents (e.g., with qualified electronic signatures/seals) meet the requirement of originality and reliability.

5. Remove or revise the requirement to verify physical security features such as holograms, especially for documents that are issued digitally or are otherwise obtained from reliable and independent sources. The current language is overly prescriptive, may not be relevant for all document types (e.g., corporate registry extracts), and risks undermining modern electronic verification practices.

Question 3: Do you have any comments regarding Article 8 on virtual IBANS? If so, please explain your reasoning.

The Association answer:

While we support the objective of ensuring that credit and financial institutions can comply with their obligations under Article 22(3) of Regulation (EU) 2024/1624, we respectfully seek clarification on the scope and format of the information to be transmitted under Article 8 of the draft RTS in the context of virtual IBAN arrangements.

In particular, we ask the EBA to confirm whether the transmission of core identification data such as name, date of birth, nationality, and identification number is considered sufficient for the purpose of enabling the credit or financial institution servicing the account to meet its obligations. We understand this to mean that supporting verification materials, such as document types, verification methods, outcomes, or scanned copies, would not need to be transmitted by default, but rather should be retained by the originating institution and made available only upon request, where necessary to evidence compliance.

We believe that this interpretation would be consistent with the proportionality and efficiency principles underpinning the EU AML/CFT framework and ensure traceability and access to verification records without unnecessarily duplicating procedures or introducing operational friction as well as avoid the unintended imposition of a "Know Your Customer's Customer" (KYCC) obligation, which would go beyond current legal requirements and established supervisory expectations.

Therefore, we kindly suggest EBA confirming that:

1. The obligation to transmit "*information for identifying and verifying the identity*" under Article 8 refers primarily to the transmission of essential customer identification data, and

2. Verification records and supporting documentation are not required to be shared proactively, but should be accessible upon request and within a timeframe that enables the receiving institution to meet its regulatory obligations.

Clear guidance on this point would promote consistent application of the RTS across Member States while avoiding regulatory overreach and undue operational burden.

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?

The Association answer:

We appreciate the EBA's efforts to provide further granularity on the application of Articles 20(1)(c) and 25 of Regulation (EU) 2024/1624. However, we respectfully do not fully agree with the proposals in Section 2 of the draft RTS, as several elements risk undermining the principle of proportionality and the risk-based approach that underpin the AMLR.

1. Lack of Differentiation Between Business Relationships and Occasional Transactions

The current draft does not clearly distinguish between the CDD expectations applicable to occasional transactions versus ongoing business relationships. In our view, the RTS largely reiterates Article 16 without adding interpretive clarity, particularly in terms of the scope and depth of information required for one-off transactions. For example, requiring customers to explain how they intend to use a product or what benefits they expect in the context of a single transaction, such as a currency exchange or one-time transfer, is redundant and may introduce unnecessary friction. We strongly recommend that the RTS explicitly recognize that occasional transactions may not warrant the same level of information collection, and that the application of these requirements should be calibrated accordingly.

2. Ambiguity of Certain Terms

We are concerned that several key terms introduced in the RTS lack sufficient definitional clarity, which may lead to inconsistent implementation:

"Benefits expected" – It is unclear whether this refers to the utility of the product, broader commercial goals, or something else entirely. **We recommend either removing this phrase or clearly defining its scope.**

"Category of funds" – This term appears in the RTS without context or definition. It is unclear whether it refers to the source of funds (e.g. salary, business income) or the type of financial instrument (e.g. savings, loan, investment). **We recommend the EBA provide a clear explanation to ensure consistent application.**

3. Overly Prescriptive and Burdensome Requirements

Several provisions within Section 2 impose detailed, prescriptive obligations that exceed both the intended scope of the AMLR and practical operational capacity. For example:

Article 15(a) introduces a requirement to determine why the customer has chosen the obliged entity's products and services. This is a commercial preference, not a risk indicator, and has limited relevance to ML/TF risk assessment. Responses are likely to be vague or unverifiable (e.g. convenience, pricing), providing little AML/CFT value while introducing unnecessary data collection and operational friction. **We recommend removing this provision or clarifying that it is only relevant in higher-risk scenarios.**

Article 15(b) requires information on the source of funds for every customer relationship. This contradicts the AMLR's risk-based model, where source of funds should be examined only where warranted by the risk profile. **We recommend removing the phrase "and their source" from this clause.**

Article 15(c) appears to impose an internal control mechanism for identifying intra-group relationships and potential conflicts of interest. While important, this level of specificity is better addressed through internal policies, not detailed regulatory mandates.

Article 16(b) demands highly granular estimations at onboarding such as the anticipated number, size, volume, and frequency of transactions. This information may not be reliably known to the customer and is impractical to assess at the outset. **We recommend that this clause be removed or revised to align with a more realistic risk-based approach.**

Article 16(e) expands the scope of occupational information collection far beyond what is typically needed for effective CDD. It calls for detailed data on a customer's sector, operations, key stakeholders, revenue streams, and more. This exceeds the AMLR requirement, which focuses on basic occupational details, and imposes a disproportionate burden. **We recommend reverting to the simpler AMLR wording.**

4. Risk of Regulatory Fragmentation

If the RTS retains highly detailed and prescriptive requirements without clarification, it may lead to divergent interpretations across Member States. Inconsistent implementation would undermine harmonization efforts and create uneven supervisory expectations.

5. Proportionality and Practical Impact

The prescriptive elements in the RTS, if adopted as-is, would result in significant operational complexity and compliance costs, particularly for institutions that onboard a large volume of retail or lower-risk customers. Many of the data points introduced (e.g. expected benefits, intermediaries used, stakeholder mapping) go beyond what is currently collected and would necessitate changes to KYC systems, onboarding questionnaires, staff training, and customer interactions, without clear evidence of improved risk mitigation.

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?

The Association answer:

We support the objective of strengthening (PEP) screening controls and appreciate the EBA's attempt to define specific procedural expectations. However, we respectfully do not fully agree with the proposals as currently drafted, due to key areas that lack clarity, raise interpretive concerns, and risk imposing disproportionate burdens that are not fully aligned with the risk-based approach. We respectfully request clarification on the intended meaning and scope of the phrase "*for the benefit of whom a transaction or activity is being carried out*". As it currently stands, this language introduces significant ambiguity, particularly in two scenarios:

a) Screening of counterparties. It is unclear whether this wording implies that counterparties to a transaction (e.g., payment beneficiaries or payees) must also be screened against PEP lists. If this interpretation is correct, it would represent a material expansion of PEP screening obligations beyond the current AMLR requirements and established market practice, significantly increasing compliance burdens.

b) KYCC obligations in pooled account scenarios. There is also uncertainty as to whether this phrase requires obliged entities to perform PEP screening on underlying clients of their customers, particularly in pooled account arrangements. If interpreted this way, it could amount to a de facto KYCC requirement. Such an expectation is not clearly supported by the AMLR and would impose a highly complex, operationally challenging, and in many cases unrealistic obligation, particularly for entities that do not have visibility into their customer's downstream relationships.

We suggest that the EBA clearly delineate the scope of this provision, explicitly stating that PEP screening applies to natural persons in a direct customer or beneficial ownership relationship with the obliged entity, and not to unrelated transaction counterparties or clients of clients.

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?

The Association answer:

We do not fully agree with the proposals in Section 4 of the draft RTS, as several provisions raise concerns regarding clarity of interpretation, legal consistency with Level 1 text, and alignment with the risk-based approach. Below we provide comments and seek clarification on specific articles within this section.

1. Verification Requirements in SDD Scenarios

The RTS remains silent on whether identity verification is required in all cases where simplified due diligence (SDD) applies. Article 33(1)(a) of Regulation (EU) 2024/1624 (AMLR) suggests that verification may be deferred for a limited time, but ultimately must be conducted. We therefore request clarification on the intended approach to verification of identity in SDD cases:

1. Should the general verification provisions (e.g., Article 5 of this RTS) apply mutatis mutandis to low-risk cases?

2. Or is it envisaged that alternative, lighter verification requirements will apply specifically under SDD?

We believe such clarification is essential to ensure consistent implementation and avoid fragmented practices among obliged entities.

2. Commercial Name Requirement in Low-Risk Scenarios

Article 18 of the RTS also introduces the requirement to obtain the commercial name of a legal entity, even in low-risk situations. However, this data point is not required by the Level 1 text of the AMLR. We respectfully suggest that this requirement be reconsidered, as it appears to go beyond the legal mandate and may be disproportionate in SDD contexts, especially where the commercial name is not relevant to risk assessment or readily available. More comments related to commercial name verification issues were also identified in other comments too.

3. Use of Data Sources for Identification and Verification of Beneficial Owners

Article 19 provides that in SDD cases, obliged entities may identify and verify the beneficial owner or senior managing officials using different sources from a defined list (points a–c). We would appreciate confirmation that:

1. It is permitted to identify the beneficial owner using one source (e.g., customer-provided statement per point b), and to verify using another source (e.g., public internet search per point c);

2. The use of the central register (point a) is not mandatory if reliable alternatives from points (b) or (c) are used, consistent with the risk-based approach.

This interpretation would allow obliged entities to apply proportionate measures suited to their specific customer profiles and product risks.

4. Interpretation of "Relevant Circumstances" in Article 22

RTS Article 22(1) outlines the conditions under which customer identification data must be updated in low-risk scenarios, including when there are "*changes in relevant circumstances.*" We seek clarification on what is meant by "*relevant circumstances*" in this context. Specifically:

1. If there are no trigger events and no suspicious or inconsistent transactions, what other changes would constitute a relevant circumstance requiring data updates?

2. Are "*relevant circumstances*" intended to refer to risk-neutral factors (e.g., change of address or legal name) or those that would trigger a re-risk assessment, thereby rendering SDD inappropriate?

We also ask whether a trigger event or an unexpected transaction would fall under the concept of "*relevant circumstances*," or whether they are to be treated as distinct triggers, as currently implied by points (b) and (c) of Article 22(1).

5. Prescriptiveness in Determining Purpose and Intended Nature of Relationship

Article 23 sets out minimum requirements to identify the purpose and intended nature of the business relationship, including the source of funds and expected transaction flows, even in low-risk cases.

We are concerned that these requirements appear overly prescriptive, potentially limiting the flexibility of the risk-based approach established in Article 33(1)(c) AMLR. In practice, certain low-risk business models inherently provide clarity on the purpose of transactions, such as:

1. Closed-loop payment systems used for low-value purchases from specific e-merchants;

2. Financial products with built-in restrictions (e.g., hard transaction value limits) that are designed to avoid ML/TF risks and promote financial inclusion.

We therefore respectfully request clarification on whether obliged entities retain discretion to calibrate the level of information collected based on actual risk, rather than being required to gather all data points in every low-risk case.

In particular, we question the requirement to establish a source of funds in all SDD cases. This blanket obligation appears to contradict the principle of proportionality and may result in a disproportionate compliance burden without corresponding risk mitigation benefits.

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.

The Association answer:

We support the inclusion of sector-specific SDD measures in the RTS and welcome the risk-sensitive approach. However, we believe further clarification is essential to ensure the proportional application of KYCC (Know Your Customer's Customer) expectations and to avoid interpretations that could lead to over-implementation or unnecessary de-risking.

1. Clarification on the Scope of KYCC Obligations

We strongly urge EBA to clarify that KYCC obligations should apply only in exceptional, high-risk scenarios, such as cases warranting enhanced due diligence (EDD), and not as a default requirement in all CDD situations. When reading the Level 1 text in conjunction with the FATF standards, we understand that KYCC requirements should only apply in exceptional circumstances, where specific ML/TF risks arise, such as in cases requiring EDD. However, as currently drafted, Article 20 and Article 21 may be interpreted to impose a blanket KYCC requirement even where ML/TF risks are demonstrably low. This would contradict the risk-based and proportionate approach embedded in both the AML Regulation and the FATF Recommendations. Such a broad interpretation risks:

1. Unnecessary administrative burden on obliged entities, including duplicative or redundant information gathering;

2. Barriers to financial access and an increase in de-risking, especially for entities unable to disclose end-client information due to legitimate confidentiality or legal constraints;

3. Potential breaches of commercial or banking secrecy laws, particularly in jurisdictions where such data sharing is restricted in the absence of ML/TF suspicions;

4. Misalignment with FATF guidance, which clearly states that financial institutions are not required to conduct CDD on the customers of their customers in correspondent relationships, unless there is a substantiated risk or concern.

We refer specifically to the FATF's Guidance on Correspondent Banking Services (Part I.A, point 2), which states:

"The FATF Recommendations do not require financial institutions to conduct customer due diligence on the customers of their customer… There is no expectation, intention or requirement for the correspondent institution to conduct customer due diligence on its respondent institution's customers."

To avoid overreach and promote regulatory clarity, we recommend that the RTS:

1. Clearly distinguish between CDD obligations towards the customer and information that may be requested about the customer's clients only where warranted by ML/TF concerns;

2. Emphasise that KYCC obligations should be triggered by risk, not applied indiscriminately;

3. Ensure that references to "being satisfied that the customer/intermediary will provide CDD information" do not imply proactive or systematic data collection on third-party clients unless required for a specific purpose (e.g. post-transaction monitoring, suspicious activity investigation);

4. Confirm that correspondent banking relationships, where properly assessed and monitored, are not subject to general KYCC requirements, in line with FATF expectations.

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?

The Association answer:

We respectfully raise the following concerns regarding the draft provisions in Section 5 of the RTS, particularly Articles 24–27, and do not fully agree with the proposals as currently formulated. Our concerns are rooted in legal clarity, operational feasibility, proportionality, and alignment with the intended scope of the Level 1 Text.

1. Departure from Risk-Based and Proportionate Approach

Similar to the concerns raised on previous sections of the RTS, the provisions in Articles 24–27 deviate from the proportionate, risk-based approach envisaged by Regulation (EU) 2024/1624. Specifically, the language "*shall at least enable*" imposes what appears to be minimum mandatory requirements, rather than a flexible framework that allows obliged entities to calibrate their EDD measures based on the specific risk context. This framing transforms what were intended as illustrative risk-based tools into de facto mandatory obligations, potentially requiring all listed assessments (e.g. points (a)–(d) of said articles) to be conducted irrespective of the actual ML/TF risk level.

We recommend that the RTS explicitly state that the measures listed are examples of possible approaches, not cumulative or mandatory in every case, thereby preserving the principle of proportionality.

2. Ambiguity from Use of "Shall at least" and "and/or"

The combined use of “shall at least” with “and/or” (e.g., Article 24(c), Article 25(b), Article 27(c)) introduces legal uncertainty regarding the scope of application: Does the provision require that all measures from - to must be applied or is it sufficient to apply only some based on a risk-based determination?

This lack of clarity undermines the intended flexibility of the framework and may lead to inconsistent application across institutions and jurisdictions. To resolve this, we recommend:

1. Removing "shall at least" and replacing it with a formulation that reinforces risk-based discretion.

2. Replacing “and/or” with either “and” or “or,” or using language such as “where relevant” or “as appropriate in light of the risk.”

3. Differentiation between obligations at onboarding and during the course of the business relationship in Article 25

This critical distinction appears to be insufficiently addressed in the current RTS draft. We therefore recommend adding explicit differentiation between obligations at the onboarding stage and those applicable during ongoing monitoring. At onboarding, obliged entities should gather adequate information to understand the anticipated use of the business relationship. In EDD scenarios, this may exceed standard CDD but still faces practical and legal limits especially due to the principle of presumption of innocence, e.g. in the case of PEPs. The RTS, as currently worded, implicitly requires a level of scrutiny at onboarding that may not be justifiable in every case, particularly in the absence of risk indicators. Thus, we recommend clarifying that:

1. EDD during onboarding should remain risk-triggered and proportionate to specific indicators (e.g. high-risk jurisdictions, complex structures, inconsistent business models).

2. Obliged entities should retain the discretion to escalate only when necessary, for instance: (i) obtaining further details on the destination of funds only if above a certain threshold; (ii) requesting business partner information only if partners raise red flags (e.g. links to adverse media or sanctions); (iii) asking for additional customer data where strictly necessary to understand the business rationale, without encroaching on commercially sensitive or GDPR-regulated data.

During the ongoing business relationship, the entity's role is to: (i) monitor transaction activity for consistency with the initial risk profile; (ii) identify new or emerging risk factors, not to retroactively re-justify onboarding information or pre-approve individual transactions.

The current formulation of point (b) implies obliged entities must verify the legitimacy of transaction recipients. This effectively expects them to act as pre-approving gatekeepers of transaction-level activity, which is disproportionate and unworkable, especially in dynamic business environments.

Therefore, we suggest EBA revise the text to clearly distinguish EDD expectations during onboarding versus ongoing due diligence and affirm the role of risk-based escalation, rather than blanket verification.

4. Article 24(5)(c) Overlap with Article 24(1)(c)

Point (c) of Article 25(1) closely mirrors the scope of Article 24(1)(c), which also addresses the need to understand the business activities of the customer or beneficial owner. We request that the EBA clarify whether the two articles are intended to address distinct assessment objectives or whether they are duplicative. If the latter, we propose consolidating or cross-referencing them to avoid redundant obligations. Furthermore, all earlier comments raised under Article 24(1)(c), particularly relating to proportionality and the risks of obliging entities to judge the legitimacy of business activities, are equally applicable here and should be reflected.

5. Additional information on the source of funds, and source of wealth in Article 26 is required

Firstly, the phrase "*shall consist of one or more of the following evidence*" suggests a closed and rigid evidentiary list. This contradicts the principle of proportionality embedded in the risk-based approach. We recommend that the RTS explicitly clarify that this list is illustrative, not exhaustive. Obliged entities must retain discretion to accept other equivalent forms of reliable documentation where appropriate to the context and customer profile. Proposed revision: "*This information shall typically consist of one or more of the following types of evidence, or other equivalent and verifiable documentation, based on the level and nature of the ML/TF risk*."

The Article 26 of RTS also introduces several undefined or vague terms such as: "authenticatable documentation"; "certified copies"; "high degree of reassurance". These are subject to varied interpretations across Member States and between institutions, potentially undermining uniformity and creating legal uncertainty. Therefore, we suggest providing clear definitions or cross-references to existing regulatory standards or EBA guidelines to harmonise implementation.

Also, the obligation to collect documentation from both customers and beneficial owners equally, regardless of the customer's structure, creates impractical expectations. In many cases, beneficial owners are not actively involved in day-to-day operations and may not be readily available for documentation. Therefore,

for beneficial owners, allow alternative forms of verification, such as confirmation from the customer entity itself, shareholder registers, or declarations from legal representatives and also recognise that direct SoF/SoW evidence may not be feasible or necessary in all cases, particularly for: (i) well-established legal entities with a long operational history; (ii) listed or regulated companies with publicly available financials; (iii) entities generating revenue from ordinary business operations.

Additional practical considerations for Article 26:

a) Point (a) – Salary Verification Requirements - the requirement for signed employer documentation is impractical and excessive in most cases, bank statements showing recurring payments with clear "salary" references should suffice.

b) Point (f) – Documentary Requirements for Asset Sales - the expectation of notarised sale contracts for routine personal assets (e.g. vehicles) is disproportionate. We suggest clarifying that such formal documentation is only required in high-risk cases, and that ordinary private contracts or transaction evidence (e.g. payment slips or declarations) may be acceptable.

c) Legal Entities – SoF/SoW from Beneficial Owners - There should be a clear distinction made: Start-ups or shell companies may justify closer scrutiny of owners' SoF/SoW. Established companies with decades of financial history and audited accounts should not trigger the same level of scrutiny into the personal finances of non-contributing shareholders or CEOs.

It seems that Article 26 requires adding language to ensure EDD obligations reflect the risk level, company maturity, and ownership structure. Avoid a blanket requirement for personal SoF/SoW data that adds no meaningful value.

6. Unclear and Overreaching Expectations in Point (a) of Article 27

Article 27(a) requires obliged entities to "verify the accuracy of the information for why the transaction was intended," which introduces an expectation to assess or even predict intent. This obligation:

1. Extends beyond the current scope of AML/CFT due diligence, which focuses on identifying inconsistencies and suspicious patterns, not verifying the subjective intent behind a transaction.

2. May be speculative and impractical in cases involving complex or indirect business models (e.g. B2B relationships, investment funds, pooled accounts).

3. Imposes a potentially unrealistic burden of proof, particularly in real-time transaction monitoring scenarios.

We recommend that this provision be reframed to focus on assessing plausibility and consistency rather than "verifying intent."

7. Scope Creep and Privacy Concerns in Point (d) of Articles 24 and 27

Several provisions (e.g. Article 24(d), Article 27(d)) suggest that in case of suspected criminal activity, obliged entities should collect additional information on: "family members, persons known to be a close

associate or any other close business partners or associates". While the objective of broadening the understanding of ML/TF risk is valid, this wording:

1 Risks expanding due diligence beyond the direct scope of customer relationships;

2. May conflict with data protection principles and privacy rights, especially where such individuals are not parties to the business relationship and where reasonable grounds for suspicion are not yet fully established;

3. Could result in significant operational challenges and data access limitations, particularly in cross-border contexts where legal thresholds for data gathering differ.

We recommend that this provision be narrowed to clarify:

- that data collected from family members and other third parties associated with customer or the beneficial owners must be limited to what is necessary for the AML purpose.

- when such information may be sought (e.g., only after suspicion is indicated and not for all EDD cases, meaning that such a requirement must remain exceptional, not systematic);

- what kind of information may be collected (e.g., identity, relationship, role in financial activities);

- how to handle cases where the customer is unwilling or unable to provide such information (to limit the risk of de-risking solely on the basis when the client is unable to provide the additional information).

8. Unclear Delegation of Law Enforcement Functions to Obliged Entities

The repeated use of language such as "verify the legitimacy/assess the legitimacy" (e.g. Article 25(a), Article 27(c)) risks blurring the lines between AML obligations and the role of law enforcement. Obliged entities are not empowered to determine the legality of transactions or business models in the criminal sense. Their role is to identify anomalies, inconsistencies, and suspicious activity that may merit reporting, not to make legal conclusions about "legitimacy."

We recommend replacing these terms with wording such as:

1. "assess the plausibility," or

2. "evaluate whether the activity is consistent with the customer profile and known business purpose."

This would better align the provision with existing AML frameworks and ensure that the role of obliged entities remains clearly defined.

9. Cost and Operational Impact

If adopted in their current form, the draft provisions in Articles 24–27 would require obliged entities to:

1. Implement significantly more comprehensive and systematic EDD checks, even in moderate-risk cases;

2. Invest in additional training, systems, and documentation frameworks to track and justify assessments of intent, legitimacy, and associations;

3. Potentially breach data protection obligations if compelled to collect sensitive information on third parties not directly involved in the business relationship.

This would result in substantial compliance costs and potential legal exposure, without necessarily yielding proportional improvements in ML/TF risk detection.

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?

The Association answer:

We broadly agree with the intention of the provisions in Section 6, which are aimed at ensuring consistency and efficiency in the application of sanctions screening measures. However, we believe that several aspects of the current drafting warrant clarification and refinement to ensure effective and proportionate implementation across diverse business models and technical environments.

1. Scope of Screening Clarification

Article 28 refers to screening of "customers and all the entities or persons which own or control such customers." While this broadly covers beneficial owners, it does not explicitly mention other categories of related parties, such as directors, authorised signatories, or senior managing officials in the case of legal entities, as well as intermediaries. So, is it correct to understand that these persons do not necessarily need to be screened, especially if there are no risk-increasing factors (e.g., in the case of low-risk customers)?

2. Transliteration Requirements

Under Article 29(a), obliged entities must screen: "... all the first names and surnames, in the original and/or transliteration of such data." The inclusion of "and/or transliteration" introduces ambiguity: Does this imply screening in both formats is required as a default expectation or is screening in only one (original or transliteration) sufficient, provided it is consistent with the technical capabilities and the underlying sanctions lists?

Furthermore, no transliteration standards are referenced. For example, multiple official ISO transliteration standards exist for Cyrillic, Chinese, Arabic, and other non-Latin alphabets, and these may not yield the same result. Sanctions lists themselves are not always consistent in transliteration format. We request that the EBA clarify which transliteration standards (e.g., ISO 9, ISO 7098, or others) are recommended or acceptable. This clarification will ensure that obliged entities can configure screening tools effectively and avoid redundant or technically infeasible configurations.

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?

The Association answer:

We generally support the principle of defining risk-reducing factors in Section 7 of the draft RTS to ensure a harmonised approach to exemptions under Article 19(7) of Regulation (EU) 2024/1624. However, we have several concerns regarding proportionality, operational feasibility, and redundancy with existing AMLR provisions. We respectfully recommend the following clarifications and amendments:

1. Transaction Value Thresholds (RTS Article 30(a)):

The requirement for low transaction thresholds is already addressed under AMLR Article 19(7), which sets a EUR 150 cap for non-reloadable payment instruments. The RTS appears to go beyond this by implying the possibility of introducing further thresholds without clearly specifying them or justifying the need. This creates regulatory uncertainty and could result in inconsistent application across Member States. To ensure coherence and legal clarity, we recommend aligning this provision strictly with the AMLR threshold and avoiding duplicative or overly vague limitations.

2. Verification of Funds Origin (RTS Article 30(b)):

Mandating that issuers verify that funds originate from an account held solely or jointly by the customer at an EEA-regulated institution introduces an additional layer of operational complexity, particularly for low-risk, non-reloadable products. These instruments are already subject to transaction monitoring requirements under the AMLR. Imposing verification of source of funds for inherently low-risk products may not provide significant additional mitigation but would increase compliance costs and onboarding friction. We recommend this requirement be reconsidered or limited only to reloadable or higher-risk products.

3. Limiting the Range of Goods or Services (RTS Article 30(d)):

Restricting the use of a payment instrument to a "very limited range" of goods or services is overly prescriptive for non-reloadable, low-value instruments. Such products already limit exposure through monetary caps and single-purpose use cases. Adding further functional constraints could reduce their utility for legitimate users without proportionally improving AML/CFT safeguards. We propose removing this clause or replacing it with a broader reference to “limited-purpose” instruments as already understood in the market.

4. Geo-Restrictions and Other Technical Measures (RTS Article 30(k)):

While geo-fencing and IP tracking can be effective in specific scenarios, mandating them across all low-risk payment instruments creates a disproportionate compliance burden. These technologies may not be feasible or necessary for issuers operating simple, offline, or single-use models. Furthermore, Article 19(7) of the AMLR does not require these tools for exemption eligibility. We suggest rephrasing this point to recommend such measures as optional safeguards, depending on the risk profile and distribution model of the product.

5. Scope of Distribution – EU-only (RTS Article 30(j)):

Restricting distribution to within the Union appears unnecessary and potentially conflicts with the practical operation of cross-border services. Provided the issuer applies adequate risk-based controls, including due diligence, monitoring, and compliance with EU AML standards, limiting availability to the EU does not substantially lower residual risk. We recommend revising or deleting this provision to allow flexibility for

products with minimal exposure and appropriate safeguards, even if some distribution occurs outside the EU.

While we understand the intent of Article 30 is to clarify risk-reducing factors for supervisory consideration, several provisions go beyond what is necessary for low-risk instruments, especially those already subject to strict value and functional limits. A more proportionate approach, focused on reinforcing existing AMLR conditions without adding unnecessary compliance layers, would preserve regulatory clarity and ensure continued access to simple, low-risk payment products across the EU. We would welcome further clarification from the EBA on how proportionality and product risk profiles will be considered in supervisory assessments under this RTS.

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?

The Association answer:

While we support efforts to define the necessary attributes for eID and trust services, the current RTS text requires clarification to ensure consistency with the AMLR. Including a reference to Article 22(7) would preserve the full spectrum of permissible verification methods, reduce unnecessary compliance burdens, and align the RTS with both the legal text and the practical realities of AML compliance namely:

1) Clarification is requested as to whether qualified electronic signatures and qualified electronic seals, as defined under Regulation (EU) No 910/2014 (eIDAS), may be used as means of remote identification and whether such use falls within the scope of this Article.

2) It is unclear from the wording of the Level 1 text whether the intention is to require that electronic identification means be used in conjunction with qualified trust services (e.g. a qualified electronic signature). The phrase "*the electronic identification means and relevant qualified trust services*" appears to suggest a cumulative requirement. Clarification is requested as to whether these two components are to be applied jointly in all cases, and, if so, guidance is needed on how such a requirement should be implemented in practice, particularly in the context of remote identification.

3) It is unclear whether, based on the wording of the RTS and the reference to Article 20(1)(b) of AMLR, it is intended that the identity of the beneficial owners must be established using electronic identification means (as a mandatory requirement for UBO identity verification). Such an interpretation would appear to extend beyond the requirements of the Level 1 text. Specifically, Article 22(6) of the AMLR provides that electronic identification means in accordance with eIDAS are to be used for the identification of the customer and, where applicable, persons acting on their behalf — but makes no such reference to beneficial owners.

Furthermore, pursuant to the applicable AMLR framework, the identification of beneficial owners requires reasonable measures to be taken, which does not necessarily imply the use of electronic identification means under eIDAS.

Additionally, we note that qualified electronic seals, as a trust service under eIDAS used for legal entities, do not contain beneficial owner-related information and therefore cannot serve as a basis for such identification.

We suggest clarifying the text.

Draft RTS under Article 53(10) of the AMLD6 on pecuniary sanctions, administrative measures and periodic penalty payments

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.

The Association answer:

No particular comments.

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.

The Association answer:

No particular comments.

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.

The Association answer:

No particular comments.

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.

The Association answer:

It remains unclear how the assessment of financial strength is intended to influence the evaluation of natural or legal persons held responsible under Articles 4(5) and 4(6), and how this interacts with the attribution of compliance failures and regulatory liability.

1. Clarification of Financial Strength as a Risk Factor

We recommend that the RTS provide a clear and proportional definition of financial strength, both in terms of what constitutes relevant financial indicators (e.g., income stability, liquidity, asset base) and how these should be assessed for natural persons (Article 4(5)) and legal persons (Article 4(6)).

In the context of natural persons, it should be clarified how financial strength is expected to correlate with ML/TF risk, and whether it is being considered as a mitigating factor or as a contributing factor to risk.

For legal persons, the RTS should specify whether financial strength refers to capitalisation, revenue scale, solvency, or operational robustness, and how this should be adjusted for newly established entities, start-

ups, or firms with non-traditional business models (e.g., Fintechs). Without such clarification, assessments may be applied inconsistently or unfairly across sectors and jurisdictions.

2. Attribution of Non-Compliance and Financial Responsibility

More critically, it remains unclear how non-compliance will be attributed and distinguished between natural persons and legal entities in practical terms. If individual accountability is to be considered, the RTS must recognize that most employees act under the instruction or governance of the legal entity, typically the Board of Directors or the CEO. We recommend that the RTS clarify the specific circumstances under which natural persons may be individually held liable, that such liability should only arise where there is deliberate negligence, gross misconduct, or intentional breach, not mere operational involvement under directive, that primary accountability should lie with senior management and governing bodies (i.e. the Board of Directors or the CEO) where failures to act (e.g., ignoring internal recommendations, delaying decisions, or failing to escalate risk issues) are evident.

3. Risk of Disproportionate Burden on AML Officers

AML/CFT responsibilities are typically distributed across multiple internal functions, including compliance, engineering, operations, customer support, and product design. Without clear delineation of roles and accountabilities, there is a serious risk that AML officers could be disproportionately held liable for systemic or procedural failures originating outside their control, especially where issues result from inadequate tooling, resourcing, or executive-level indecision.

The RTS should explicitly acknowledge this division of responsibilities and provide guidance on how regulators and institutions should assess causality and accountability before assigning liability to a specific individual or function.

4. Accountability of Third-Party Providers and Auditors

We also recommend that the RTS address the accountability of external vendors, technical service providers, and auditors, whose actions or omissions can materially affect an institution's compliance posture. For instance, sanctions screening providers failing to update lists, technology vendors delivering non-compliant or unfit-for-purpose systems, auditors providing insufficient or misleading guidance.

Currently, institutions bear the full burden of such failures, despite lacking direct control in many cases. We propose that the RTS include minimum expectations, due diligence standards, and liability frameworks for such third parties to ensure shared accountability and a more equitable distribution of compliance risk.

Question 5: Do you have any comments or suggestions on the proposed criteria to be taken into account by a supervisor when applying the administrative measures listed under this draft RTS and in particular when the supervisor intends to:

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?

The Association answer:

No particular comments.

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

The Association answer:

No particular comments.

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

The Association answer:

No particular comments.

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.

The Association answer:

No particular comments.

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.

The Association answer:

Currently, Articles 4(5) and 4(6) of the draft RTS refer to natural persons held responsible without clearly distinguishing between:

1. Natural persons engaged in financial activity in their own capacity (e.g., informal money remitters), and

2. Natural persons acting on behalf of a legal person, such as members of senior management or the management body as defined in the AMLR.

We recommend that the RTS explicitly clarify which category of natural persons it is referring to and under what circumstances each may be held accountable. This is critical for legal certainty and proportional application of regulatory expectations. The RTS should also integrate the AMLR definitions of Article 2 (1), namely: management body (p. 37), management body in its management function (p. 38), Management body in its supervisory function (p. 39), Senior management (p. 40).

Given the layered nature of decision-making and control, the RTS should distinguish between decision-makers (e.g., members of the management body or senior management with actual decision-making power), and operational staff or compliance and AML officers acting under direction. Individual accountability should only apply to natural persons in senior roles where there is clear evidence of willful misconduct, gross negligence, or intentional disregard of compliance obligations or that natural person had the authority and capacity to mitigate the risk but failed to act.

The current draft RTS risks overextending liability to AML officers or function-level employees who do not fall under the AMLR definition of senior management but may nonetheless be seen as "natural persons" involved in compliance. To address this, the RTS should include indicators for assessing the individual's proximity to decision-making and their role-specific responsibility, e.g.: did the individual have independent authority to act? was the individual part of a governing or executive decision-making body? Was the failure caused or exacerbated by executive inaction, governance failure, or systemic process breakdowns?

Therefore, we propose that the RTS include a tiered framework of natural person categories (e.g., individual financial operators, senior management, employees), examples of when individual liability applies, based on governance role and responsibility, a requirement to consider the governance structure and whether the root cause of failure lies at the management body level, not with individual staff, exclusion of liability for actions carried out in good faith under instruction from higher governance levels.

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?

The Association answer:

Currently, the draft RTS lacks sufficient detail on how periodic penalty payments are to be determined in practice. This can lead to inconsistent application across competent authorities, and legal uncertainty for obliged entities and natural persons. A more structured and transparent methodology would support consistency across Member States, especially for cross-border institutions, predictability for supervised entities, allowing for better compliance planning, proportionality and fairness, by ensuring penalties are appropriately scaled. To achieve these objectives, we recommend that the RTS include a structured list of factors to guide both the imposition and calculation of penalty payments.

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?

The Association answer:

Currently, the draft RTS does not provide a harmonised set of administrative rules for the imposition of periodic penalty payments. This may result in divergent practices across Member States, creating legal uncertainty and an uneven supervisory landscape. Introducing more structured and harmonised rules at EU level would promote consistent enforcement, enhance legal clarity, and ensure a fair and proportionate approach for all obliged entities, particularly those operating across borders.

To support this, we recommend that the RTS explicitly allow for administrative settlement arrangements, similar to those applied in Lithuania, where supervised entities that admit non-compliance and demonstrate cooperation may benefit from a reduction in penalty payments. Such provisions should specify the conditions for settlement, including maximum discount thresholds, procedural safeguards, and criteria such as early admission and corrective action.

Further, the RTS should set out minimum procedural guarantees, including clear notification processes, timelines for response, and appeal rights, to ensure fairness and transparency. It should also require that cooperation efforts (e.g. voluntary disclosure, timely remediation, and good compliance history) be taken into account when determining the amount and duration of penalty payments.

Finally, the RTS should establish transparent publication rules for such decisions, clarifying when anonymisation is permitted, to reinforce accountability while protecting legitimate interests.

We consider that inclusion of these administrative provisions in EU legislation would better serve the goal of harmonisation than leaving them to national discretion.