

3 September 2026

EBF feedback on AMLA draft guidelines on ongoing monitoring of a business relationship under Article 26(5) of Regulation (EU) 2024/1624

Question 1: Do you consider that Guideline 1 supports a risk-based approach and clearly sets out the core principles that obliged entities should apply to keep customer information up to date?

If you see scope for further clarification, please:

(i)specify the paragraph concerned;

(ii)explain your rationale; and

(iii)consider submitting an amendment proposal

Limit: 3,000 characters for rationale, additional 3,000 characters for amendment proposals (optional) (max 20 comments)

Comment 1 - Key terminology is not defined or explained

Rationale

Several key terms are used without being defined in the AMLR or these Guidelines (GLs) or otherwise explained. This creates legal uncertainty and makes it difficult to assess how the GLs relate to the Level 1 text. Examples include:

- "Continuous monitoring" (paragraph 59): the distinction between continuous, real-time and ongoing monitoring is unclear.
- "Activities" / "transactions and activities": article 26 AMLR refers only to "transactions" and does not refer to "activities". The Guidelines appear to broaden the scope by introducing the concept of "activities", while "transactions" itself is still not defined.
- "Enhanced scrutiny" (paragraphs 40-41, 78): The AMLR defines "enhanced due diligence"; the relationship between "enhanced scrutiny" and EDD is unclear.
- "Default settings" (paragraph 50): obliged entities must assess and calibrate "default settings" of monitoring tools, but the term is not defined (thresholds, scenarios, rules, parameters?).
- "Reference or peer groups", "(aggregated) expected transaction profile", "expected behavioural profile", "customer-group profiles" (paras 53-56): these terms are used as concepts, but none of these terms are defined nor properly explained.
- "Without undue delay" is used as the standard for assessing and resolving monitoring outputs and managing backlogs, but no timeframe is given (contrary to several articles of the AMLR that use this terminology). Additionally, in paras 18 and 20 "without delay" is used. We suggest that AMLA replace this with "within a reasonable timeframe".

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu

Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23


www.ebf.eu

- “Material ML/TF risk indicators” (paragraph 78) is not defined nor explained.
- “Model risk” (paragraph 89): obliged entities must take “model risk” into account, but the term, and the related concepts of bias, robustness and transparency, are not defined nor explained.
- The Guidelines refer to “supervisory authority” whereas the AMLR’s defined term is “supervisor”.
- “Identification data” (paragraph 21): it is unclear what is covered by “identification data”.
- The Guidelines should consistently distinguish “periodic review” from “data actualisation” (keeping information up to date) and similarly, “review” and “update” are used as synonyms whereas these terms reflect different concepts.

Amendment Proposals

We ask AMLA to define these terms and align them with the AMLR (defined) terminology, and to confirm they do not expand beyond Level 1 obligations.

Comment 2 – Paragraph 3

Rationale

While supporting the risk-based approach set out in paragraph 3, we believe that an increase in a customer’s risk should not automatically trigger a requirement to collect additional information when the information already held is adequate and remains sufficient to assess and mitigate the identified risk.

Amendment proposal

Where the customer’s risk has increased, obliged entities “may” obtain any additional information if the information already available is not sufficient to assess and apply appropriate risk-mitigating measures, including enhanced measures where higher risks where identified.

Comment 3 - Paragraph 6

Rationale

Paragraph 6 requires obliged entities to ensure that the outputs of their monitoring framework are assessed and used to inform internal processes. However, it is unclear which “internal processes” are meant and how the monitoring outputs should feed into them. Depending on the interpretation, this could include updating customer risk profiles and CDD, recalibrating monitoring scenarios and thresholds, informing the business-wide risk assessment, or supporting FIU reporting. Greater clarity would promote consistent implementation and avoid divergent supervisory expectations.

In addition, Paragraph 6 should clarify that only risk-relevant and assessed monitoring outputs may inform a customer’s risk classification.

Using all monitoring outputs indiscriminately risks creating a self-reinforcing risk increase: monitoring hits lead to a higher customer risk classification, which in turn leads to more

intensive monitoring and further hits. This may result in a disproportionate number of customers being classified as high risk without a corresponding increase in the underlying ML/TF risk.

Changes to the customer's risk classification should therefore be based only on validated, material and customer-relevant findings, rather than on unreviewed monitoring alerts.

Amendment proposals

AMLA should specify in Paragraph 6 which internal processes are referred to and clarify that this feedback loop should be applied on a risk-sensitive basis.

We suggest rewording Paragraph 6 as follows: "... Where appropriate, risk-relevant and sufficiently substantiated outputs may be used to inform updates to customer due diligence information and the customer's risk classification.

Comment 4 - Paragraph 8

Rationale

We support the objective of ensuring appropriate governance, traceability and accountability. However, the requirement to document any limitations arising from the nature of the business, all related mitigating measures and resulting monitoring outcomes appears to be overly broad and may create disproportionate documentation requirements. Documentation should focus on limitations that are material and relevant to the ML/TF risks being mitigated.

Amendment proposal

The requirement should be limited to documenting material limitations relevant to the ML/TF risks being mitigated arising from the nature of the business, the mitigating measures applied to address those limitations, and the resulting monitoring outcomes where material to the effectiveness of the ongoing monitoring framework.

Comment 5: Paragraph 12

Rationale

The current wording appears to limit acceptable sources to the categories listed under points (a)–(e). In practice, obliged entities may also rely on analytical models and internal data-driven approaches to assess certain customer attributes (e.g., residency or activity patterns inferred from transactional behaviour, particularly in cases of customer non-response). These sources do not clearly fall within the listed categories, creating uncertainty as to whether their use is permitted.

Par. 12(c) refers to "*information or confirmation provided directly by the customer, either in writing or through digital means*". In practice, obliged entities also obtain a significant amount of information directly from customers through other forms of interactions with customers, including meetings and telephone conversations. Paragraph 12(c) should

therefore explicitly recognise information obtained through direct interactions more generally, rather than being limited to information provided "*either in writing or through digital means*", particularly where the AMLR does not require supporting evidence.

In addition, Paragraph 12(c) allows customer-provided information to be used where it is of "sufficient quality", but this concept is not defined and may be subject to divergent interpretations across obliged entities. This creates uncertainty as to the level and type of evidence required (e.g., self-declarations, screenshots, scans, uncertified copies) and could result in operational inefficiency such as unnecessary follow-ups and over-collection of documentation without a corresponding risk-based benefit. It may also incentivize obliged entities to adopt conservative, document-heavy approaches, including for lower-risk updates, contrary to the intended risk-based approach.

Amendment proposals

We would suggest considering the following two options:

- We would suggest removing Paragraph 12 in its entirety, as the requirements regarding the sources and updating of customer information are already addressed in the CDD RTS.
- If retained, we would suggest replacing the current wording with the following: "Customer information sources should include, where relevant and appropriate, one or more of the following:". Moreover, AMLA should explicitly expand the list or add a broader category to accommodate analytical models and internal data-driven approaches used to assess certain customer attributes (while maintaining appropriate safeguards).

Comment 6: Paragraph 14 - Some customer information can only come from the customer

Paras 12 and 14 introduce the concept of "reliable and independent sources" to update the customer information and require from the obliged entities to assess the reliability and independence of the information source without defining it. Further clarification would be helpful on this concept to ensure consistent interpretation across institutions and avoid overly conservative approaches, especially in low-risk scenarios.

More specifically, Para. 14 provides that, where information is provided by the customer, the obliged entity should consider whether the reliability of that statement needs to be verified using independent and reliable sources. We support this risk-based approach to verification. The Guidelines should, however, also acknowledge that certain information can, by its nature, only be obtained from the customer, as no independent or reliable external source may be available to corroborate it. In such cases, the customer's statement that has been assessed for plausibility and consistency, may constitute the only available source, and the absence of independent verification should not, in itself, be treated as a shortcoming.

It may be also useful to clarify that, for ongoing due diligence purposes, obliged entities may rely on their own assessment of whether the customer relationship remains consistent

with their knowledge of the customer. Where ongoing monitoring provides sufficient comfort that the information held and the customer's activities remain consistent with the obliged entity's understanding of the relationship, it should not always be necessary to contact the customer solely to reconfirm information already held.

Amendment proposals

EBF requests that AMLA consider deleting reliability provisions in Paragraph 14 of these Guidelines, provided that equivalent provisions are retained in the final CDD RTS. This would avoid duplication, ensure consistency across instruments and keep the verification requirements within the scope of the CDD mandate.

If Paragraph 14 is retained, the concepts of “necessary knowledge” and “power of representation” should be clarified, as their current wording may lead to inconsistent interpretations across obliged entities. Customer information is frequently obtained, confirmed or updated through face-to-face interactions, telephone conversations or other established channels, rather than through written statements by the customer. Furthermore, once a person's authority to act on behalf of a customer has been appropriately established and verified, obliged entities should be able to rely on existing records unless there are specific circumstances that call that authority into question.

EBF also suggests clarifying in Para. 14 that, where no independent and reliable source is reasonably available, the obliged entity may rely on the information provided by the customer, subject to a risk-based assessment of its plausibility and consistency.

This is particularly relevant in the context of complex international ownership structures, trusts, foundations, or jurisdictions where reliable and independent beneficial ownership information is not reasonably available - requiring independent verification in all such circumstances would create disproportionate operational burdens and inconsistent supervisory expectations. In these cases, obliged entities should be able to rely on customer-provided information, provided that: (i) reasonable verification steps have been undertaken and documented; (ii) no material inconsistencies or indicators of unreliability have been identified; (iii) the information is assessed as plausible and consistent with the obliged entity's understanding of the customer and the business relationship; and (iv) any residual risk is appropriately reflected in the customer risk assessment and ongoing monitoring measures. The absence of independent verification should not, in itself, be considered a deficiency where no reliable and independent source is reasonably available.

Finally, consistent with EBF's request under paragraph 12c regarding recognizing obtaining information based on face-to-face customer interaction as an acceptable source alongside written and digital means, EBF requests removal of “a written statement with”.

Comment 7: Paragraphs 16 - 18:

Rationale

Paras. 16–18 suggest that expired identity documents may need to be re-collected based on factors such as the issuing country, time elapsed since expiry or outdated security features. While we support the principle that expired identity documents should not be re-collected by default, we caution that the extensive list of factors in Para. 17 may introduce unnecessary complexity and should be applied strictly on a risk-based basis. Once a customer's identity has been reliably established, it remains established: mere expiry or the absence of certain security features should not, in itself, trigger re-collection.

Core identification data rarely changes, and many factors listed in Para. 17 may have limited relevance to the customer risk assessment. The assessment should therefore be data-driven and risk-based, rather than document-driven. Re-collection should be required only where there is a concrete ML/TF risk, a material change in relevant identification data, or a specific doubt as to the accuracy or reliability of the information held. In particular, point c) refers to the length of time since the document expired. In the absence of any indication of what period should be considered relevant, this criterion may lead to arbitrary and divergent outcomes across obliged entities. Similarly, point e) requires OEs to assess whether a newly issued document would provide updated or additional relevant information. This may be difficult to determine, particularly for foreign identity documents, where obliged entities may not have sufficient knowledge of their content. Point e) should therefore not be mandatory. Unnecessary re-collection will create adverse customer experiences and impose additional operational costs. Moreover, factors such as the "risk associated with the issuing country" could give rise to discriminatory outcomes and should therefore be applied with caution. Furthermore, in a growing number of MSs, obliged entities have access, directly or through authorised intermediaries, to official population registers, civil registries or equivalent governmental databases. Where updated identification data can be obtained and verified directly from an official and reliable government source, re-collection of a newly issued identity document should not be required unless it provides additional information necessary for AML/CFT purposes. Requiring customers to provide a replacement document where equivalent information is available from an official governmental source would create unnecessary customer friction and costs, and would be inconsistent with the principles of proportionality, simplification and data minimisation. Finally, customer age and the ability to visit a branch or submit documentation through digital channels should be considered when determining whether a renewed identity document should be obtained. This is relevant for elderly or otherwise vulnerable customers assessed as low risk based on the other relevant risk factors.

Amendment Proposals

Updating an identity document is relevant where there are doubts as to the continued accuracy or reliability of the customer's identification. In the absence of such doubt, previously obtained identity documents should remain sufficient for review purposes.

EBF suggests removing from Paragraph 16-18 factors such as the country of issuance, time elapsed since expiry and lack of up-to-date security features, and requiring re-collection only where there is a risk-relevant trigger or a specific doubt as to the accuracy or reliability of the customer's identification. Paragraph 17 should be reworded as follows :

"On a risk-based approach, obliged entities should assess whether or not an expired identity document, passport or equivalent needs to be updated where there are doubts as to the accuracy of the customer's identification data held or suspicions of ML/TF. The assessment may take into account the following non-exhaustive factors:"

We propose either deleting point (c), so that the assessment focuses on relevant customer and geographical risk factors, or specifying a reference period, e.g. one year after expiry.

We also propose deleting point (e) or qualifying the requirement by adding "where possible".

This should be extended to (d) as well.

We also suggest referring to the comment already submitted by EBF in the context of the RTS CDD consultation: "Once identified, always identified": once a customer has been properly identified in accordance with applicable standards, re-verification should not be required solely because an identity document has expired. Such a requirement would create an unnecessary operational burden without strengthening AML/CFT safeguards and could disproportionately affect vulnerable customers.

We propose the introduction of a new provision in Paragraph 17:

"Whether updated identification data can be obtained directly from reliable and independent official sources, including population registers, civil registries or equivalent governmental databases, without requiring the customer to provide a newly issued identity document."

Consequently, we propose adding the following provision:

"Where updated identification data can be obtained from reliable and independent official sources, obliged entities should be permitted to update the customer information on the basis of such sources without necessarily re-collecting the newly issued identity document, unless there are doubts as to the customer's identity or the authenticity or reliability of the information obtained, or there are ML/TF concerns."

Comment 8: Paragraphs 19–21

Rationale

We understand from the "Background and rationale" section that a standard periodic review may not always be appropriate for certain business models, particularly where a business relationship exists but no new activity or services are provided over an extended period.

The draft GLs maintain periodic review requirements while allowing some adaptation based on risk. However, they do not clearly allow for automated recertification or “perpetual KYC” for low-risk customers.

More specifically, Para. 19 states that “periodic reviews should always be conducted” in accordance with Article 26(2) AMLR. However, Art. 26(2) concerns the actualisation of customer information and the requirement to keep such information up to date. This should be distinguished from performing a full periodic review. Keeping customer information up to date does not necessarily require a full periodic review. This distinction should be made explicit and applied consistently throughout the GLs. Art. 26(2) only sets maximum intervals for updating customer information, while continuous monitoring and event-driven reviews can ensure that information remains current within those intervals.

Paras. 19–21 should be amended to confirm that, under the RBA, customers may be exempt from full periodic reviews where no material change or triggering event has occurred.

In addition, the interpretation of “within one year” in the context of periodic reviews requires clarification. It is unclear whether the requirement is for the review to be fully completed within the one-year period or whether the timeframe is intended to allow a reasonable period to conduct the review in practice. AMLA is invited to clarify whether initiating the review within the specified timeframe would be sufficient to meet the requirement.

We recommend that the GLs further promote a risk-based, perpetual KYC model rather than calendar-driven periodic reviews. In an effective AML/CFT framework, customer information is kept current through continuous, trigger-based monitoring and event-driven reviews, rather than time-scheduled reviews of the entire client portfolio, particularly for low-risk customers.

The GLs should clarify that periodic review requirements can be fulfilled through continuous monitoring, screening and trigger-based reviews, and that a risk-based review may legitimately conclude that no update is necessary where continuous monitoring has identified no relevant change or trigger. OEs should also have sufficient flexibility to keep customer data up to date using reliable or official sources, including relevant internal data. Where such data provides sufficient assurance that existing customer information remains accurate, unnecessary customer outreach should not be required.

These clarifications would prevent periodic review from being interpreted as requiring a systematic full KYC refresh where customer data remains current and unchanged.

Amendment Proposals:

- Clarify in Paragraph 19 that data actualisation may be carried out in the manner most appropriate to the obliged entity, within the applicable deadlines, using reliable, formal or official sources and relevant internal data, without necessarily requiring customer outreach.

- State that the periodic review requirement may be satisfied through documented continuous and trigger-based monitoring and that a separate periodic review is not required where no relevant changes or triggers have been identified.
- Confirm whether “within one year” requires the periodic review to be completed within that period or whether it is sufficient for the review to be initiated within the applicable timeframe.

EBF also suggests adding this section to paragraph 20:

“Where a customer is classified as low-risk and no triggering event within the meaning of Article 26(3) AMLR has occurred, the periodic review referred to in Article 26(2) AMLR may be conducted through an automated recertification process. This approach should apply horizontally to all categories of obliged entities referred to in Article 3 of the AMLR, irrespective of sector, and without prejudice to the obligation to conduct an event-driven review where a triggering event under Article 26(3) AMLR occurs. In such cases, the review should be limited to the data or information directly affected by the triggering event, without requiring a full recertification of the entire KYC file.”

Comment 9: Unusual transactions -paragraphs 15 (34, 47, 60, 61, 62, 68, 69, 71, 74, 78)

Rationale

Throughout the Guidelines, the term “unusual transaction” is used, whereas Article 69 AMLR requires the reporting of “suspicious transactions”. While the concept of “unusual” transactions appears in the AMLR in the context of the “detection of unusual or suspicious transactions” (Articles 18, 19, 33), the Guidelines should clarify the purpose of using the term “unusual transaction” and its relationship with the Level 1 suspicious transaction reporting requirements.

In addition, Paragraph 15 unnecessarily duplicates an obligation already clearly established in Article 69 AMLR.

Proposed amendment

EBF proposes removing Paragraph 15 and clearly link “unusual transaction” to the detection and not to the reporting duty.

Comment 10: Paragraph 22:

Rationale

Paragraph 22 states: “Obliged entities may use the transaction or activity history to determine whether the source of funds remains consistent...”. Transaction history may assist in assessing whether customer behaviour remains consistent with the expected profile. However, transaction monitoring alone cannot generally confirm or validate the source of funds. The wording risks conflating source of funds verification with behavioural monitoring and may create unrealistic supervisory expectations.

Amendment Proposals

We propose the following rephrasing: "Obligated entities may use transaction or activity history to assess whether the customer's behaviour remains consistent with the expected customer profile and previously established source of funds information."

Comment 11: Paragraphs 24 to 29

Rationale

We suggest clarifying paragraphs 24–29 to avoid creating a de facto perpetual KYC model that is not aligned with the distinct requirements for periodic reviews under Article 26(2) AMLR and event-driven reviews under Article 26(3) AMLR.

In particular, Paragraph 28 could be interpreted as requiring continuous automated monitoring of all potential changes in customer information. This raises the question of the purpose and scope of the periodic review cycle if customer information is expected to be continuously identified, assessed and updated in any event. We would like to emphasize that manual or semi-automated controls may be equally appropriate where they effectively identify relevant changes in customer identification and are proportionate to the obliged entity's business model. The Guidelines should therefore clarify that the appropriateness of controls should be assessed based on their effectiveness in managing the risks of ML/TF rather than on the degree of automation used.

The Guidelines should clearly distinguish between the two types of review. An event-driven review should be limited to the specific trigger and its potential impact on the customer's ML/TF risk. Where, however, an event-driven review covers the same scope as a periodic review or where several event-driven reviews cumulatively cover all aspects of a full review, this should be recognised as fulfilling the periodic-review requirement and reset the relevant review cycle. Otherwise, obliged entities may be required to conduct duplicative reviews with overlapping scope and timelines. This would be inconsistent with a risk-based, proportionate or simplified framework and result in an inefficient allocation of resources.

Amendment Proposals

We suggest amending paragraph 28 in the following way: "Having regard to the nature, risks and complexity of their business, as well as their size and business-wide risk assessment, obliged entities should assess whether automated or semi-automated systems and processes are appropriate to support the timely detection of relevant trigger events. Such systems and processes should be proportionate and should not require the continuous collection, verification or updating of customer information in the absence of a relevant trigger event or other risk-based justification."

We also suggest adding the following section: "Where an event-driven review covers the same scope as a periodic review under Article 26(2) AMLR, it should be recognised as fulfilling the periodic review requirement and reset the relevant review cycle. Where an

event-driven review is limited to the matter that triggered it, obliged entities should assess and update only the customer information relevant to that trigger and its potential impact on the ML/TF risk of the business relationship.”

Comment 12: Paragraph 25

Rationale

Paragraph 25 requires relevant changes related to the customer to be detected, reviewed and addressed without undue delay. However, certain changes may not be reported by the client and may therefore not be immediately detectable. For example, a customer who becomes a PEP may not be under an obligation to inform the obliged entity of that change.

Furthermore, the time taken to review and manage these changes depends on the staff dedicated to process these alerts, on the number of alters to manage and on the time taken to find up-to-date information (which may depend on the client’s answer time).

Amendment proposal

It would be more appropriate to replace the concept of “without undue delay” by “within a reasonable timeframe”.

Comment 13: Paragraph 27

Rationale

EBF considers para. 27 overly broad regarding the circumstances requiring ODD. The new event-triggered ODD requirements are disproportionate and may impose continuous monitoring obligations that are neither proportionate nor risk-based. AMLA should clarify that the listed events are risk-based examples and do not require continuous checks across the customer portfolio where not warranted by the customer’s risk profile or product. An event-triggered review should assess the specific trigger and its implications and should not automatically require a full review of the customer’s risk profile.

Point (a): it is unclear what is meant by “changes in identity”. Core identity elements are generally stable. AMLA should clarify that sufficient assurance on identity does not require each customer attribute to be independently verified. The trigger concerning “authorised signatories or representatives” should be limited to persons authorised to legally represent or bind the customer pursuant to a proxy agreement or power of attorney, and should not cover employees acting in the ordinary course of employment (e.g. senior managers, treasury or relationship management staff).

Point (b): it is unclear whether OEs are expected to continuously monitor “repeated or unusual changes in IP address or device location”. For many OEs and products, such information is unavailable or of limited relevance to ML/TF risk. Such monitoring may raise GDPR data minimisation and proportionality concerns and impose disproportionate costs. Indicators that a customer is abroad may reflect legitimate circumstances such as travel, remote working, mobile networks or VPN use and should be interpreted with caution. Such indicators should trigger further assessment only where relevant to the customer’s risk.

Point (c): should not require continuous adverse media screening across the entire customer base, which would impose a significant operational burden and is not aligned with the RBA. Moreover, “material change” is not defined.

Point (d): further clarification is needed to ensure proportionality. It should not require continuous requests for financial or tax information to detect changes in financial situation. Changes in financial circumstances, products used or engagement with higher-risk jurisdictions do not, in themselves, indicate increased ML/TF risk. In line with Para. 21(c), a new product or service should not automatically trigger an information update, but only where it carries materially higher inherent ML/TF risk or fundamentally alters the nature of the relationship.

Trigger events should not automatically evidence increased ML/TF risk or require a full customer-file review. OEs should assess whether a trigger is material, reliable and relevant, and determine the proportionate review scope. Automatic full KYC refreshes would generate low-value reviews and divert resources from material risk changes.

Proposed amendments

- EBF proposes clarifying in Paragraph 27 that the listed events are risk-based examples, and that the manner and frequency of detection should follow the obliged entity’s risk-based approach, depending on the context, client type, products and nature of the business relationship, rather than requiring continuous monitoring of each listed element for every customer.
- EBF proposes clarifying that an event-driven review can be limited to the assessment of the trigger event and does not require a full review of the customer risk profile when there is no reason to review other information. Obligated entities should assess the materiality, reliability and relevance of the event, as well as its actual impact on the customer’s ML/TF risk profile, in order to determine the scope and depth of any review required.
- EBF proposes replacing in Paragraph 27 a) “authorised signatories or representatives” with “the persons authorised to legally represent or bind the customer pursuant to a proxy agreement or a power of attorney”.
- EBF proposes removing paragraph 27 b) and 29 b) as their application could lead to important risk of tipping off, which is forbidden by the AMLR.
- 27 d): EBF proposes amending Paragraph 27(d) as follows: "Changes in financial situation, source of funds or wealth or business activity that deviates from the customer’s profile or from the expected purpose and intended nature of the business relationship: significant variations in financial standing, financing structures, asset composition or control, adoption of new products or services that carry a materially higher inherent ML/TF risk profile or fundamentally alter the intended nature of the business relationship, or engagement with higher-risk jurisdictions or counterparties".

Where the legal representative is not a beneficial owner, is not subject to enhanced due diligence measures, is not a politically exposed person and no specific risk indicators are identified, information concerning that individual’s personal wealth should generally fall outside the scope of information necessary to assess the customer’s source of funds,

ownership and control arrangements, or the ML/TF risks associated with the business relationship.

Comment 14: Paragraph 30: Inability to update information should not be equated with inability to apply CDD

Rationale

Paragraph 30 requires obliged entities that are “unable to keep the relevant customer documents, data or information up to date” to refrain from transactions and ultimately terminate the relationship. This appears to equate an inability to update information with the situation in Article 21 AMLR, where an entity is unable to apply CDD measures. These situations should be clearly distinguished: an inability to refresh a specific item of information does not necessarily mean that the obliged entity is unable to apply CDD measures and should not automatically trigger the consequences set out in Article 21 AMLR.

We would also point out that financial institutions may be subject to contractual or other legal obligations that may affect their ability to implement suspension, restriction or termination measures. Obligated entities should be permitted to take such obligations into account when determining the applicable measures. In particular, certain regulated securities and asset management services provided to EU-regulated funds (e.g., custody/custodianship, fund administration, transfer agency services) may not be legally capable of being suspended or terminated on this basis alone, given applicable sectoral requirements and investor-protection obligations, including under UCITS and AIFMD). Suspension or termination may be permissible only in specific circumstances, such as targeted financial sanctions or instructions from competent authority. The current wording may therefore create legal uncertainty and potential conflicts between AMLR requirements and applicable sectoral fund regimes.

As drafted, Paragraph 30 therefore lowers the threshold for serious consequences such as transaction restrictions and account termination, which may lead to financial exclusion, adverse customer outcomes or perceived discrimination, and may sit uneasily with the right to a basic payment account under the Payment Accounts Directive (PAD¹). At the same time, the possibility of suspending or blocking transactions should be preserved where justified by a relevant risk trigger, for example where a customer fails to respond to an information request. We therefore ask AMLA to align Paragraph 30 with Article 21 AMLR and to clarify that such measures may be applied only where they are proportionate and taken risk-based basis.

Amendment Proposals

- Align Paragraph 30 with the wording of Article 21 AMLR, clarifying that the obligation to refrain from carrying out transactions and to terminate the business relationship

¹ Directive 2014/92/EU

arises only where the obliged entity is unable to comply with the application of customer due diligence measures, rather than merely because a particular item of information cannot be updated.

- Delete or amend the restriction in Paragraph 30 to ensure that the suspension or blocking of transactions remains available as a risk-based measure in response to a risk trigger, e.g., where a customer fails to respond to a request for information.

This is particularly important where termination would have disproportionate consequences for the customer - for example, in relation to mortgage products, pension schemes, or other products that are of fundamental, long-term importance to the customer, as well as for large and complex customer relationships. In such cases, and absent any suspicion of ML/TF, obliged entities should not necessarily be required to terminate the relationship, but should instead be able to apply proportionate risk-mitigating measures, such as restricting the relationship, refraining from providing new products or services, or limiting access to certain functionalities until the outstanding issues are resolved.

- Clarify in Paragraph 30 that any suspension, restriction or termination must be proportionate and without prejudice to applicable sectoral legislation for regulated funds and securities services. Suggested wording: "Obliged entities should take into account applicable legal and regulatory constraints before considering any suspension, restriction or termination of the business relationship."
- Add a safeguard regarding the duration and review of restrictions, as follows: "Any such restrictions should be temporary, proportionate and subject to periodic review, and should not be maintained for longer than necessary to obtain the required customer information."

Comment 15: Paragraphs 30 and 33 – interaction with the Payment Accounts Directive

Rationale

Although Paragraph 33 refers to the interaction with the (PAD), it does not provide practical guidance on how an obliged entity should reconcile its obligation to suspend or terminate a business relationship due to a lack of updated customer information with the customer's right of access to a basic payment account. Further clarification on the interaction between these requirements and the PAD would therefore be helpful to ensure a consistent and legally sound application by obliged entities.

Amendment Proposal

AMLA should include an explanatory box illustrating how obliged entities should reconcile the suspension or restriction measures under Paragraph 30 with the right of access to a payment account with basic features under the PAD, particularly in relation to consumer customers.

Comment 16: Paragraph 4: Scope of “activities, behaviours and events”

Rationale

Paragraph 4 states that ongoing monitoring should not be limited to transaction monitoring but should also capture relevant activities, behaviours and events throughout the business relationship. While we support a holistic view of the customer, the terms “activities, behaviours and events” are very broad and, without boundaries, could be interpreted as extending monitoring to conduct unrelated to the business relationship, which, without appropriate boundaries, would also risk colliding with the data protection principles. AMLA should clarify that this concerns only activities, behaviours and events that occur during the business relationship between the obliged entity and the customer.

Proposed amendment

Paragraph 4 should be amended to clarify that ongoing monitoring must be conducted in a risk-based and proportionate manner and should capture relevant activities, behaviours and events within the business relationship, that is, those carried out by or on behalf of the customer during that relationship pertaining to the role of the obliged entity and information reasonably available to the obliged entity.

Question 2: Do you foresee any challenges in applying Guideline 1, taking into consideration the differences in obliged entities’ nature, risks and complexity of their business, as well as their size?

If you see scope for further clarification, please:

(i) specify the paragraph concerned;

(ii) explain your rationale; and

(iii) consider submitting an amendment proposal

Limit: 3,000 characters for rationale, additional 3,000 characters for amendment proposals (optional) (max 20 comments)

Comment 1: Paragraphs 19 and 20

Rationale

Para. 19 establishes a general expectation that OEs adjust the depth and intensity of periodic reviews on a risk-sensitive basis, including when determining which information, data or documents require updating.

We understand Para. 20 as providing for reduced depth and intensity of periodic reviews in lower-risk cases. However, the drafting appears to conflate the general obligation with the approach tailored to low-risk cases. For example, point (a) requires OEs to consider the customer’s risk level when determining the depth and intensity of the review, whereas the main paragraph refers specifically to low-risk customers. Systematically, the list of factors should therefore be included in Para. 19 rather than Para. 20.

The restriction of simplified review approaches to low-risk customers may unduly limit the application of a genuinely risk-based approach. We recommend deleting “for low-risk customers”. Where the nature and pattern of the business relationship remain materially unchanged, OEs should be able to determine the appropriate scope and intensity of the periodic review based on the risks and circumstances of the relationship. This flexibility should apply to customers subject to both reduced and enhanced due diligence, provided no new type of activity has occurred and no new products or services have been offered.

Moreover, Article 33(1)(d) AMLR already provides for a generally reduced scope and intensity of periodic reviews for low-risk customers. Para. 19 should therefore articulate the general risk-based approach, allowing OEs to calibrate reviews according to the customer’s risk profile and the characteristics of the business relationship.

The wording of Para. 20 could also suggest that reduced-depth and reduced-intensity reviews apply primarily to dormant accounts. This extends to points (b) and (e), which refer to “new activity or transaction”. We understand the intended reference to be a new type of activity, rather than individual transactions or activity as such. The wording should be clarified accordingly.

The Guidelines should further clarify that simplified periodic reviews do not necessarily require systematic customer outreach or full re-verification of all customer information. OEs should determine, on a risk-sensitive basis, which information, data or documents require updating and the appropriate means of doing so.

Finally, we understand from the “Background and rationale” section that a standard periodic review may not always be appropriate where a business relationship continues over an extended period without material change in the nature of the activity or products or services provided. We welcome this approach, which supports efficient and proportionate reviews and is consistent with technological solutions and automated monitoring. Given its practical importance, this principle should be expressly reflected in the Guidelines.

Amendment Proposals

EBF proposes moving the factors listed in points (a) to (e) to Paragraph 19 and adding the following clarification:

“For low-risk customers, the periodic review obligation may be fulfilled through an automated or semi-automated recertification process where reliable internal or external sources, together with ongoing controls, provide sufficient assurance that no material change has occurred in the customer’s key customer due diligence information or ML/TF risk profile. Such an approach should ensure an appropriate audit trail and provide for escalation to a targeted or full review where a material change or relevant exception is detected. A periodic review should not, in itself, necessarily require renewed customer outreach or a new end-to-end manual review of the customer file.

Furthermore, we suggest clarifying in Paragraph 19 that obliged entities may adjust the depth and intensity of periodic reviews on a risk-based basis for customers subject to reduced due diligence and enhanced due diligence, where no new type of activity has

occurred and no new products or services have been offered. The factors (b) and (c) set up in this paragraph should be therefore reworded as follows:

"b) Whether new activity or transaction has occurred or new services or products have been offered to the customer and whether, despite the absence of new product or services, the risk profile does not justify reducing the depth and intensity of monitoring.

c) The type and risk level of products or services provided to the customer".

Finally, in points (b) and (e), references to "new activity or transaction" should be replaced with references to a "new type or nature of activity".

We also suggest adding the following within Paragraph 20:

"Where a business relationship continues over an extended period without any new type of activity or any new products or services being provided, obliged entities may determine, on a risk-based basis, that a standard periodic review is not necessary and may instead rely on effective on-going controls, including screening, transaction monitoring and event-driven reviews. Obligated entities should be able to demonstrate that such an approach is proportionate to the AML/CFT risks associated with the business relationship, taking into account the characteristics of the obliged entity. This rationale for the approach should be duly documented by the obliged entity".

Comment 2: Depth and intensity of periodic reviews Paragraphs 20(b), and 20(e)

Rationale

We ask AMLA to revise Paragraph 20 so that obliged entities may reduce the depth and intensity of reviews across all risk levels, rather than only for low-risk customers without new activity. "Low risk" and "no activity" should not be the only determining factors to reduce the depth and intensity of a review. Moreover, even where AMLA provides a "non-exhaustive list of factors", this might become a checklist. It would be therefore preferable to allow obliged entities to determine, on a risk-based basis, and taking into account the customer profiles and products, whether and how to adjust the depth and intensity of periodic reviews. Relatedly, applying EDD measures does not automatically mean that a customer is classified as high risk; we ask AMLA to clarify this distinction.

Paragraph 20 currently presents the factors for adjusting review depth and intensity mainly in the context of low-risk customers. Moving factors a)-e) to Paragraph 19 would help clarify that these factors support a risk-based assessment across all risk levels.

Paragraph 20(b) requires obliged entities to consider whether any new activity or transaction has occurred or new services or products have been offered to the customer. On the other hand, point e) refers to new activity or transaction initiated by the customer or by third parties, in which case a review should be carried out without delay.

For banks this factor is not workable as customers and third parties initiate transactions continuously. This element would in practice turn every transaction into a periodic review and undermine the risk-based approach the Guidelines intend to support.

We note the apparent overlap of scope between points (b) and (e). The factors (b) and (c) are mixing existence of new activities with the risk level of products and services.

Moreover, both points (d) and (e) of Paragraph 20 refer to conducting a review “without delay”. This seems to imply that these factors are considered as trigger events as per Section 2.4. However, no reference is made to the latter section. Paragraph 26 of Section 2.4 already requires a risk-based scope for trigger-based updates.

The reference to “transaction” in point (e) also appears inconsistent with the beginning of the paragraph, which refers only to “activity” “services” and “products”. This could potentially result in an disproportionate operational burden, particularly given the requirement to carry out this review without delay.

We also note that points (d) and (e) seem to correspond only to the trigger events listed in Paragraph 27(d), and not the ones in points (a) to (c) of this paragraph. In parallel, point (d) refers to trigger events as a whole. We believe that, in principle, all reviews should be covered by the general provision of Paragraph 19, in line with Section 2.4.

Proposed amendments

- Delete from Paragraph 20 element (e): “whether a new activity or transaction is initiated by the customer or by third parties”.
- Avoid mixing “low-risk customer” with simplified measures and clarify that applying EDD measures does not automatically mean that a customer is classified as high risk.
- Merge points (b) and (e) of Paragraph 20 into point (d): “whether any event listed in Paragraph 27 has occurred which warrants a review of the customer’s information according to the obliged entity’s assessment”.
- Move the factors listed in Paragraph 20 (a)-(e) to Paragraph 19, so that they apply to reviews across all risk levels.
- Clarify that “new activity” in Paragraph 20 refers to a new type of activity, so that the provision is not read as referring to dormant accounts only.

Comment 3: Paragraphs 20-21

Rationale

The ability to adjust the depth and intensity of the review where “no new activity” has occurred presupposes a consolidated customer-level view across all business relationships and products. In large financial institutions, however, the same customer may hold multiple products or use different service channels supported by separate systems. Consolidating this information is not always technically feasible in real time, creating a risk of incorrectly classifying a customer as having “no new” activity.

Amendment Proposal

AMLA should clarify that, for obliged entities offering multiple products or services through separate systems, the assessment of “no new activity” under Paragraph 20 should be based on a documented, periodic reconciliation across relevant systems, rather than

requiring real-time aggregation, provided the obliged entity can demonstrate that its process reliably captures cross-product activity within a reasonable timeframe.

Comment 4: Data does not expire absent a trigger (Paragraph 19-21)

Paragraph 19-21 imply a recurring re-assessment of documents, data and information at each periodic review. However, this appears as contradictory with Paragraph 19 which already requires obliged entities to determine the depth and intensity of updates based on the customer's overall risk profile which is more in line with the risk-based approach principle. Within an effective control framework, supported by reliable detection systems, the correctness of verified customer data does not expire until there is a concrete reason to doubt it. Updating is then driven by events, not by the calendar. This minimises unnecessary customer outreach. The fixed AMLR timeframes can remain the legal backstop, but where ongoing monitoring or an event-driven reviews confirm that customer information remains accurate and up to date, this should be sufficient for the review cycle.

We request AMLA to confirm that within an effective control system, periodic reviews of Paragraph 19-21 can rely on banks' own analysis and monitoring, without periodically contacting the customer, and that no re-assessment is needed when monitoring has flagged no triggers. The "age" of a document should not in itself be a determining factor.

Where customer identification information can be verified through reliable and independent sources, including official registers, public databases, or other authoritative sources, obliged entities should not be required to re-obtain identification documents unless there are reasonable grounds to believe that the information is inaccurate, incomplete, outdated, or otherwise unreliable.

Proposed amendments

- AMLA should state in Paragraph 19 that verified data remains valid until a risk-relevant event is triggered and that periodic customer information requests are not required where reliable monitoring is in place.
- We suggest the removal of paragraph 21: EBF agrees that the categories listed in paragraph 21 are relevant elements of customer due diligence. However, the Guidelines should avoid prescribing a fixed list of customer information that must be assessed in every periodic review. The introductory wording already requires obliged entities to determine the scope of updates by reference to the customer's overall risk profile, which is consistent with the risk-based approach under the AML/CFT framework. Obligated entities should therefore retain discretion to determine which information, documents or data require updating, based on their risk assessment, ongoing monitoring and understanding of the customer relationship. Hence we suggest removal of paragraph 21.
- If retained, in order to prevent the review of these elements from becoming a bureaucratic exercise, the wording of para. 21 should clarify that obliged entities may determine for themselves which information or documents should be updated. We suggest the following amendment to this point: "When determining which documents, data, or information need to be updated as part of a periodic review,

obliged entities should assess the information collected at customer onboarding and during the most recent customer review. Obligated entities should make a risk-based assessment to determine the appropriate scope of updates, taking into account the customer's overall risk profile".

Comment 5: Paragraph 29

Rationale

The scope of application of Paragraph 29(c) is unclear. The AMLR does not provide for any obligation to consult registers, except, where applicable, when establishing a business relationship. Therefore, there appears to be no basis for consulting registers in order "to detect" changes. Therefore, it would be necessary to clarify in the Guidelines that it's only when obliged entities are aware of a change by the customer or during a periodic review of the customer that the review is triggered. Indeed, we are concerned that the point a) of the Paragraph 27 in combination with the Paragraph 29 c) might be interpreted to imply that a change within a register must trigger a review, even though the obliged entity is not necessarily aware of this change, as it is under no obligation to check the register regularly. Indeed, Paragraph 29 c) imply that obliged entities may refer to "company registries and public databases to detect changes".

Amendment proposals

We propose to clarify in point (a) that only the changes in identity, legal status or ownership known by the obliged entity could trigger a review ("Changes in identity, legal status or ownership known by the obliged entity).

In addition, Paragraph 29 could be interpreted as if it excludes information that has been provided directly on an ad-hoc basis rather than during the usual course of communication. We suggest explicitly including it in the wording of Paragraph 29(g) or removing during the usual course of communication.

We further propose clarifying that discrepancies identified between customer-provided information and information obtained from company registries, beneficial ownership registers or other reliable official sources under Paragraph 29(c) should be assessed on a risk-based basis, having regard to their materiality and potential impact on customer identification, beneficial ownership determination and the ML/TF risk assessment. Not every discrepancy should automatically require a full customer review.

Comment 6: Paragraph 31

In our view, the mere absence of transactions or activities does not, in itself, give rise to additional ML/FT risk, since dormant accounts are already being monitored. Measures are in place to safeguard such accounts. In any case, customer data would be updated before new transactions are permitted.

Comment 7: Paragraph 32

We would welcome clarification that “repeated and reasonable steps” can include digital outreach, automated reminders, self-service portals and scalable communication channels. To avoid legal uncertainty, we would also appreciate clarification on how the rules regarding suspension/restriction measures relate to payment account access obligations.

Comment 8: Paragraph 33

Rationale

A common scenario is one in which the obligated entity wishes to terminate a business relationship but is unable to do so due to contractual or other overriding legal obligations. In such cases, it is often not possible to conduct a KYC procedure, as the customer typically does not provide the necessary data and this information cannot be obtained from external sources either. In these instances, there is a need to reduce the frequency and depth of the periodic review.

Amendment Proposals

We suggest adding the following sections:

“In exceptional circumstances where an Obligated Entity is unable to terminate a business relationship without breaching binding contractual obligations or exposing itself to material litigation risk (for example, in the case of committed credit facilities, revolving facilities, or other long-term contractual arrangements where no event of default or other contractual termination trigger has occurred), the obliged entity may, on a risk-based and exceptional basis, suspend or significantly reduce the frequency and depth of periodic reviews of customer information, provided that all of the following conditions are met and documented:

(a) All transactions and activities unrelated to the specific contractual obligations giving rise to the inability to terminate (hereinafter referred to as the “sticky asset”) are blocked or otherwise suspended;

(b) No new products, services, or additional facilities are offered or made available to the customer;

(c) The obliged entity maintains effective, documented controls capable of promptly detecting any material change in the customer’s activity, behaviour, profile, beneficial ownership, or risk factors;

(d) The obliged entity continues to perform ongoing and real-time screening for targeted financial sanctions and any other mandatory monitoring requirements applicable to the remaining activity linked to the sticky asset; and

(e) The obliged entity has assessed and documented that the measures in lit. (a) to (d) are sufficient to effectively manage the money laundering and terrorist financing risks associated with the business relationship.

The obliged entity should regularly reassess, at appropriate intervals, whether the conditions set out above continue to be met and whether termination of the business

relationship has become feasible. Where termination becomes possible, the obliged entity shall terminate the relationship without undue delay.

The decision to apply the above measures, the supporting assessment, and the controls implemented shall be documented and made available to competent authorities upon request. The application of this exception does not relieve the obliged entity of its obligation to report suspicious activity in accordance with Article 69 where relevant indicators arise.”

Question 3a: Compared to your current ongoing monitoring process, what impact would Guideline 1: Keeping customer documents, data or information up to date have on your compliance costs and operational processes? Please provide the estimated percentage increase or reduction in annual compliance costs:

One option has to be chosen below:

- ☐ Increase of compliance costs and operational processes
- ☐ Reduction of compliance costs and operational processes
- ☐ No effect

Sub question 3a*: Increase/Reduction

One option has to be chosen below:

- ☐ Below 25%
- ☐ 50-75%
- ☐ More than 75%

Sub question 3a: Please explain the basis for your assessment, including the methodology used and any supporting evidence:**

N/A

Question 3b: Please rate the expected impact (very positive; positive; neutral; negative; very negative) on the following operational processes:

	Very positive	Positive	Neutral	Negative	Very negative
periodic customer information review including document re-collection	☐	☐	☐	☐	☐
event-driven reviews;	☐	☐	☐	☐	☐
implications for staff;	☐	☐	☐	☐	☐
Other (please specify)	☐	☐	☐	☐	☐

Other (please specify below):

Sub question 3b*: If you selected “negative” or “very negative” for any of the above under 3(b), please explain the basis for your assessment, including the methodology used and any supporting evidence, and indicate the distinction between one-off investment costs and recurring costs.

N/A

Question 4: Do you foresee any challenges in applying Guideline 2? In your view, does the guideline provide sufficient clarity, remain proportionate, and ensure applicability across your products and services to support effective, risk-based monitoring of unusual or suspicious transactions and activities?

If you see scope for further clarification, please:

(i) specify the paragraph concerned;

(ii) explain your rationale; and

(iii) consider submitting an amendment proposal

Limit: 3,000 characters for rationale, additional 3,000 characters for amendment proposals (optional) (max 20 comments)

Comment 1: Paragraph 79

Rationale

Paragraph 79 refers to “the review of potential cases where suspicious transactions or activities were not identified”. This wording may be interpreted as creating an expectation that obliged entities identify and review all potential false negatives generated by their monitoring framework. Such an expectation would be impractical and could create uncertainty as to the standard of effectiveness expected of transaction monitoring systems and controls. The focus should instead be on appropriate quality assurance activities designed to identify possible detection gaps through risk-based testing and sampling.

Amendment Proposal

We suggest amending the Paragraph 79 as follows:

“Obliged entities should ensure that the underlying decision logic can be understood and documented. They should also ensure that the effectiveness of automated mechanisms is subject to effective human oversight, including periodic quality assurance testing, including, where feasible and proportionate, reviews of samples of cases to identify potential detection gaps.

Comment 2: Paragraphs 34 (a) (b) (c), e): holistic monitoring and data availability.

Rationale

Para. 34(a) refers to the Payment Services Regulation (PSR), which is not yet finalised, so OEs have no visibility on its impact on the monitoring framework. We suggest clarifying that references to Regulation (EU) 2023/1113 and the PSR apply only where relevant and applicable to the OE’s business model, products, services and risk profile. Not all OEs are subject to these requirements or have access to the related payment or crypto-asset

transfer data. The wording should therefore not create an expectation to establish controls that are inapplicable or disproportionate.

Re (b): Para. 34(b) requires monitoring data to be “timely”. This may mean real-time, near-real-time or periodically refreshed data. It should be clarified that timeliness is assessed on a risk-sensitive and proportionate basis, taking into account the OE’s business model, products, services, operational role, data availability and ML/TF risks.

As similarly put forward in the consultation on the RTS under Articles 16(4) and 17 AMLR, the requirement to include group information under Para. 34(b) should remain subject to relevance, reliability, legal permissibility, data availability, purpose limitation, confidentiality and operational feasibility. OEs should determine on a risk-based basis which internal, external and group-level information is appropriate and proportionate, without being required to systematically obtain all potentially available group information.

Regarding Para. 34(c), EBF supports a holistic understanding of customer behaviour. However, references to “complete, accurate and timely data” and “all products and services” could be interpreted as requiring an immediately available, fully integrated single customer view across all products, systems, entities, business lines and jurisdictions. Monitoring should instead be risk-based, focusing on higher-risk products and services and relevant indicators for lower-risk products (e.g. anticipated loan repayment). Covering all products and services may be disproportionate where they do not materially contribute to ML/TF risk. The scope should focus on products and services relevant to detecting unusual or suspicious activity.

Para. 34(e) appears to require continuous detection of changes in ownership or control structures. Such changes are generally identified through periodic or event-driven KYC reviews and, where appropriate, reliable external sources. The Guidelines should clarify that real-time detection is not required and that a risk-based approach applies. Para. 34(e) should also distinguish party screening (e.g. intermediaries, ownership/control structures and counterparties) from transaction screening or monitoring (e.g. assets and transaction patterns), as these controls rely on different data, systems and processes.

Amendment proposal

EBF proposes amending Paragraph 34(a) as follows:

a) “Leverages, where applicable and proportionate, systems and processes required under other Union legislation, such as Regulation (EU) 2023/1113 or the payment services framework”

EBF proposes amending Paragraph 34(b) as follows:

“Relies on data that is sufficiently complete, accurate and timely for the intended monitoring purpose, taking into account the materiality of documented data limitations and the ML/TF risks being mitigated, drawing on sources available to the obliged entity and, where relevant, information lawfully exchanged within the group pursuant to Article 16(3) of AMLR.”

EBF proposes amending Paragraph 34(c) as follows:

“Covers, on a risk-based and proportionate basis, the products and services that are relevant to the customer’s ML/TF risk profile and for which sufficiently reliable and usable data is available, in order to enable a holistic understanding of the customer’s behaviour and support the detection of unusual or suspicious transactions and activities.” EBF also proposes adding:

“Where legal restrictions, data availability or system architecture prevent immediate full integration, obliged entities may apply a phased approach supported by documented limitations, risk-based prioritisation and appropriate mitigating controls. The requirement should not be interpreted as a general obligation to aggregate or share all customer, product or behavioural data across entities, business lines or jurisdictions.”

EBF proposes amending Paragraph 34(e) as follows:

“Is capable of identifying, through appropriate party screening and, where applicable, transaction monitoring, patterns, behaviours or linkages that may indicate risks related to the non-implementation or evasion of targeted financial sanctions ...”

Comment 3: Monitoring framework to be “based on” the business-wide risk assessment (par. 46)

Rationale

Paragraph 46 then asks obliged entities to use the BWRA to assess whether their manual processes and controls are sufficient. This presents the relationship as one-directional, with the BWRA used only to design or justify controls. In practice the relationship is bidirectional: the BWRA informs the monitoring framework, but it is also the instrument used to assess how effective and sufficient the controls already in place are. AMLA should describe this as a two-way, iterative relationship.

Proposed amendment

AMLA should reword Paragraph 46 to clarify that the BWRA both informs the design of the monitoring framework and is used to assess the effectiveness and sufficiency of the processes and controls already in place.

Comment 4: Paragraph 35

The wording of Paragraph 35 could be interpreted in different ways. On one hand it could be seen as only relevant for obliged entities that, by nature of their business model, have limited or no access to transaction or activity data. On the other hand, it could be read as applying to financial-sector obliged entities within banking groups where monitoring or data processing is centralised. The Guidelines should clarify that such group arrangements may be relied upon where effective monitoring, information sharing, escalation and local oversight are ensured.

Comment 5: Paragraph 37

The Guidelines would benefit from greater alignment with the draft RTS on Group-Wide Requirements and additional measures for subsidiaries and branches in third countries under Articles 16(4) and 17(3) AMLR.

Clarification is needed regarding how obliged entities should incorporate group-wide risk information, monitoring outcomes and customer intelligence into ongoing monitoring processes to ensure a consistent and consolidated approach to ML/TF risk management across the group, particularly given there may be variation in the risk posed by group entities' respective products, services and distribution channels.

Comment 6: Paragraph 39

The examples of "more complex products, services, or business models" listed in Paragraph 39 do not appear to be intrinsically related and do not seem to require the same level of monitoring effort. We would like to point out that the extent to which sophisticated analytical monitoring techniques are used in individual cases should depend on the respective obliged entity's role, business model, data access, legal constraints, products, services, and ML/TF risk exposure.

Comment 7: Paragraphs 38, 43, 44, 53

Rationale

The Guidelines set minimum conditions for the monitoring framework that appear disproportionate.

Paragraph 38 refers to intermediaries without defining it, leading to confusion regarding the notion of underlying customers. If the underlying customer gives orders to the intermediary which then proceeds to the operations in the obliged entity's books, then the regular transaction monitoring process will capture the operation already.

Paragraph 43 provides that "Obliged entities should ensure that their monitoring framework is capable of identifying and assessing without undue delay new ML/TF methods, trends and typologies". However the adaptation of the monitoring framework requires time for the modification of configuration in order to optimize its effectiveness. Separately, Paragraph 43 could also be read as imposing a research obligation to identify new ML/TF trends and typologies, going beyond a risk-based monitoring framework; the intended obligation is presumably to stay informed of trends already identified by supervisors and FIUs and to incorporate them where risk-relevant, not to identify new trends independently.

As currently drafted, Paragraph 44 does not reflect this principle. We therefore recommend explicitly reflecting this principle in the wording of this paragraph. For instance, patterns are very difficult to assess in the context of wholesale banking.

Amendment proposals

EBF encourages AMLA to provides more proportionality in the context of the transaction and activity monitoring framework general considerations and include references to the risk-based approach.

For instance:

- regarding timing consideration in Paragraphs 43 and 53, the term “undue delay” should be replaced by “reasonable timeframe” ;
- regarding detection of risks in Paragraph 44, replace “Obligated entities should ensure that their monitoring framework is capable of detecting ML/TF risks that only emerge when transactions and activities are considered together over time, rather than in isolation. This includes but is not limited to” with “Obligated entities should ensure that their monitoring framework is capable of detecting ML/TF risks that only emerge when transactions are considered together within a reasonable timeframe, rather than in isolation. This may include on a risk-based approach, but is not limited to.....”

Regarding Paragraph 43, the wording should also be clarified to confirm that the obligation is to stay informed of ML/TF trends and typologies already identified by supervisors and FIUs and to incorporate them into the monitoring framework where risk-relevant, rather than to identify new trends independently.

Comment 8: Paragraph 42

Rationale

We support the principle that obliged entities should document the design and effectiveness of their monitoring framework. However, the documentation requirement should be aligned with these overarching principles. The additional, more prescriptive requirements on documentation dilute this principle without providing added value. We therefore recommend limiting the documentation requirements to the high-level principles set out in the proposed wording set out below.

Amendment proposals

EBF proposes to amend Paragraph 42 as follows: “Obligated entities should implement a monitoring framework that is appropriate to their size, nature of business, transaction volumes, complexity and ML/TF risk exposure. The monitoring framework should be risk-based and reflect the risks identified in the business-wide risk assessment. Obligated entities should document the design and effectiveness of their monitoring framework and be able to demonstrate both to the competent authorities upon request”.

Comment 9: Paragraph 49

Rationale

We recommend explicitly incorporating the principle of proportionality into paragraph 49 and including a cross-reference to the overarching principles set out in paragraph 42. This would ensure that the requirements are applied in a manner commensurate with the

obliged entity's size, risk profile and the nature and complexity of its business, while maintaining consistency throughout the Guidelines.

Amendment Proposal

Obligated entities should maintain, and where needed, calibrate their monitoring framework to ensure that it remains effective and produces valid and risk-relevant and reliable output, in a manner commensurate with their size, risk profile and the nature and complexity of their business.

Comment 10: Paragraphs 51(-57)

Rationale

While institutions are investing in more integrated monitoring framework, the implementation approaches differ significantly, reflecting variations in business models, technology environments, legacy systems and organizational structures. Achieving such integration is a multi-year transformation program for most institutions with significant costs.

Instead, greater clarity would be beneficial regarding the practical expectations associated with integrated Ongoing Monitoring. In particular, institutions would benefit from a clearer understanding of the expected role and impact of the holistic customer view, the interaction between monitoring systems.

The Guidelines should remain technology-neutral and define the expected outcomes that integrated Ongoing Monitoring frameworks are expected to deliver.

In particular, Paragraph 51 appears overly detailed. If retained, it should clarify that “integrated and coordinated” does not require full technical integration or automated data flows between all CDD, sanctions screening and monitoring systems. In practice, obliged entities may use separate specialised systems, for example for transaction screening, name screening and case management. Effective coordination can also be achieved through documented governance arrangements, alert-handling procedures, escalation processes and qualified staff assessments.

The requirement should remain risk-based and proportionate to the nature, size and complexity of the obliged entity, as well as to its ML/TF and sanctions risks. Where a relevant alert or risk indicator is identified, the necessary link between CDD and the monitoring framework may be ensured through timely manual intervention, including event-driven reviews, risk-rating adjustments, enhanced due diligence, escalation, restriction or termination of the relationship, and reporting where appropriate. The Guideline should not imply a requirement for mandatory end-to-end automation or system-to-system feedback loops.

Amendment Proposals

EBF encourages AMLA to supplement Paragraphs 51–57 with additional guidance describing the expected outcomes of integrated Ongoing Monitoring, while clarifying that

institutions may achieve these outcomes through different operating models, governance arrangements and technology solutions.

Proposed amendment to par. 51: “Obligated entities should ensure that their customer due diligence processes, including sanctions screening processes, and their monitoring framework operate in a coordinated, proportionate, risk-based manner, taking into account the nature, size and complexity of their business. Such coordination, including information sharing and escalation, may be achieved through technical integration or through documented procedures, effective governance, alert-management processes and timely intervention by qualified staff. This includes ensuring that the relevant documents, data or information are complete, accurate and up to date in accordance with the requirements set out in Guideline 1.

Paragraph 57 should clarify that only those discrepancies or inconsistencies that are material and, following the assessment of the obliged entity, constitute a possible basis for suspicion of ML/TF or related criminal activity will lead to a reassessment.

Comment 11: Peer-group monitoring and expected transaction profiles (Paragraph 53-55)

Paragraph 53-54 allow obliged entities to use reference or peer groups and an aggregated expected transaction or activity profile, and to calibrate monitoring to that baseline. We welcome this, because grouping customers and working from an expected transaction profile is a risk-based and efficient common practice in the banking industry and focuses resources where the risk is highest.

To better reflect the risk-based approach underpinning the Guidelines, we suggest amending Paragraph 53 by adding the wording “prioritised based on risk” alongside “within a reasonable timeframe”. This would clarify that deviations from a customer’s known or expected transaction, activity, behaviour or risk profile should be identified and assessed within a reasonable timeframe, with priority given to higher-risk deviations. This would ensure consistency with Paragraph 75 and with the general risk-based approach set out in Paragraph 25. It would also recognise that monitoring frameworks generate alerts of differing relevance and risk, which should be handled according to a documented risk-based prioritisation process.

With regard to the safeguards in Paragraph 54-55: every deviation must be assessed against the individual customer's profile, the absence of a deviation at peer-group level cannot on its own dismiss an individual indicator, and peer groups may not be relied on where customer behaviour is heterogeneous. Read strictly, these could require case-by-case manual handling that removes the efficiency that group-based monitoring is meant to provide. We ask AMLA to confirm that these safeguards can be met through proportionate, risk-based processes (including automated and group-level handling) and do not require a manual, individual review of every deviation from a peer-group pattern.

Proposed amendments

- Proposed amendment to Paragraph 53: “Monitoring should be calibrated to this baseline so that deviations from the customer’s known or expected transaction,

activity, behaviour or risk profile can be identified in a reliable manner and within a reasonable timeframe, prioritised based on risk”.

- Clarify in para 54-55 that the individual assessment may be carried out in a risk-based and proportionate way, so that peer groups and expected transaction profiles remain usable as an efficient monitoring tool, provided that individual risk indicators which are triggered are still assessed on their own merits.

Comment 12: Paragraph 58

Rationale

Paragraph 58 states that ongoing monitoring is performed on a continuous basis throughout the business relationship but it would be useful to indicate that it is also performed on a risk-based approach.

Amendment proposals

We propose the following amendment: “obliged entities should, as a general rule, ensure that ongoing monitoring is performed on a continuous basis and a risk-based approach throughout the business relationship”.

Comment 13 Paragraphs 60 and 61 (60-67)

Rationale

Art. 26 AMLR does not establish a general obligation for pre-transaction, pre-activity or real-time monitoring. Art. 26(1) requires ongoing monitoring of business relationships, “including transactions undertaken” by the customer, referring to transactions already undertaken rather than requiring assessment or intervention before execution. Paragraphs 61–62 should therefore not be read as requiring ex-ante monitoring wherever an OE has the technical ability to assess, delay or stop a transaction. Such an interpretation would go beyond Article 26, the risk-based approach and the mandate of a Level 3 instrument.

Given its legal, operational and technological implications and implementation and maintenance costs, any general pre-monitoring obligation should have a clear mandate in Level 1 legislation, rather than being introduced through guidelines. While ex-ante monitoring may be warranted where required by a competent authority, FIU or other legal obligation, or for specific products or business lines where risks are better addressed before execution, OEs should retain discretion, based on their business-wide risk assessment, to determine which risks are best addressed before execution and which can be managed through post-transaction monitoring.

Paras. 60–67 should not establish a general expectation of pre-transaction or real-time monitoring wherever technically possible. Certain products and payment services are subject to strict execution timelines and other legal requirements limiting the ability to delay, interrupt or review transactions before execution. Paragraph 61 could require substantial changes to operating models, processing architecture and customer journeys,

significant investment and ongoing maintenance. A predominantly ex-ante AML/CFT framework would also be impractical, as alerts require analysis against the customer profile, transaction history and wider activity. Systematically blocking or delaying transactions pending such analysis would significantly affect customers and require substantial additional staffing.

A general pre-transaction or real-time monitoring obligation would also not be compatible with Reg. 2024/886 on instant credit transfers in euro (IPR), as OEs cannot realistically reconcile its execution timelines with general pre-transaction monitoring.

A general pre-monitoring requirement would have significant customer consequences, particularly in technology-driven, non-face-to-face services where customers expect transactions to execute instantly. Delaying or blocking transactions could also alert customers that a transaction is under review, potentially compromising investigations or raising tipping-off concerns.

Pre-execution controls already exist in defined high-risk areas, including fraud prevention, sanctions screening and counter-terrorist-financing controls. A general ML/TF pre-transaction mandate would substantially overlap with these safeguards, while increasing compliance costs and alert volumes.

Amendment Proposals

In light of the considerations set above, we proposed that paragraphs 60–67 be removed in their entirety.

If retained, we propose the following amendment to paragraph 61: “Based on the findings of their business-wide risk assessment, obliged entities should determine which categories of transactions or activities present risks that are more effectively identified and mitigated prior to execution. Where, taking into account their role, business model and access to relevant information, obliged entities have the ability to assess or intervene prior to a transaction or activity being carried out or completed, they should apply pre-transaction, real-time or pre-activity monitoring to those categories of transactions or activities.”

Comment 14: Paragraph 71

Rationale

We believe the concept of “undue delay” is not operationally workable in all cases, as some monitoring tools are intentionally designed to generate alerts on a periodic (e.g., monthly) basis where this is proportionate and better aligned to the underlying activity (for example, to detect meaningful patterns, aggregated flows or cumulative risk indicators, and to avoid excessive false positives); in these cases, alert generation on a monthly cycle is not a “delay” but a risk-based design choice, and the expectation should focus on timely assessment once outputs are available, rather than implying near-immediate generation.

Amendment proposal

Replace “without undue delay” in Para. 71 with “within a reasonable timeframe (commensurate with the nature, risk and design of the monitoring framework and the availability of relevant data)”, to preserve proportionality and technological neutrality while still ensuring prompt investigation and escalation once alerts are produced.

Comment 15: Paragraph 72 and 73

Rationale:

To better reflect the risk-based approach underpinning the Guidelines, we suggest clarifying that post-transaction monitoring should be conducted not only "within a reasonable timeframe" but also in a manner that is prioritised based on risk. This would ensure consistency with Paragraph 75, as well as with the general risk-based approach set out in Paragraph 25.

As noted in our comments on Paragraph 66, the supervisory expectation and in par. 73 in particular, the intended hierarchy between pre-activity and post-transaction monitoring are not sufficiently clear. We would therefore welcome further clarification to ensure a consistent understanding of the expected monitoring approach, particularly in light of different payment execution models, such as instant payments.

Amendment Proposals:

EBF suggests to amend Paragraph 72 by adding the words "prioritised, based on risk," alongside " within a reasonable timeframe" to clarify that, where post-transaction monitoring is required, obliged entities should ensure that appropriate monitoring measures are applied within a reasonable timeframe and prioritised based on risk, taking into account the nature, timing and completeness of the information available.

EBF suggests revising wording of Paragraph 73 to better explain the intended relationship between pre-activity and post-transaction monitoring, ensuring that the supervisory expectations are applied consistently across different payment execution models, including instant payments.

Comment 16: Paragraphs 75 – 76

Rationale

Paragraph 75 states that obliged entities should ensure that monitoring outputs are resolved without undue delay. However, if the assessment of the nature of the output is possible without undue delay, it is not possible to resolve the alert without undue delay because these alerts require a certain amount of time to be analyzed, particularly when they relate to complex transactions.

Obliged entities should ensure that monitoring outputs, whether generated through automated systems or arising from manual processes within the monitoring framework, are assessed in a timely and risk-based manner, prioritised according to their nature, materiality and associated ML/TF risk, and, where appropriate, escalated for further

analysis to staff with suitable expertise and knowledge of the customer or business relationship.

It is important to note that the requirement to process requests “without undue delay” can only apply to first-level processing. Furthermore, in some national legal systems, the concept of “without undue delay” is interpreted as a fixed and very short timeframe. Applying this standard to the complete resolution of monitoring outputs could therefore create unintended operational challenges and would not be appropriate for complex cases.

The concept of “without undue delay” may only serve as a prerequisite for the initial assignment of a monitoring output within a prioritization process. While the subsequent in-depth review of the specific case should take place in a timely manner, it may take longer or shorter. We ask that this be clarified in the Guidelines text.

As already noted in our comments on Paragraph 72, EBF would welcome clarification that monitoring outputs should not only be assessed within a reasonable timeframe but also prioritised based on risk. This would better reflect the risk-based approach and enable obliged entities to allocate resources proportionately to higher-risk alerts and cases.

Amendment proposal

EBF suggests revising wording of Paragraph 75 to clarify that monitoring outputs, whether generated through automated systems or manual processes, should be assessed within a reasonable timeframe and prioritised based on risk, taking into account their nature, materiality and associated ML/TF risk. The Guidelines should also distinguish the initial assessment and prioritisation of monitoring outputs from their subsequent investigation and resolution, recognising that the latter may require additional time, particularly for complex cases. The same clarification should be reflected in paragraph 76.

Comment 17: Paragraph 78 - Automated decisions and automation of processes

Rationale

The draft Guidelines appear to introduce significant restrictions on automated decision-making.

The main concern is that the draft Guidelines could be interpreted as restricting the use of automation beyond certain stages of alert processing, particularly for decisions involving higher-risk customers. This is particularly relevant given the automation initiatives currently being developed across the European financial industry. As currently drafted, the Guidelines could be read as allowing automation only at Level 1, while excluding automation for both investigation and decision-making at Level 2/Level 3.

Such an interpretation could conflict with ongoing programmes, including AI-supported closure of cases where no suspicious activity report is filed.

Additional wording should therefore be introduced to preserve sufficient flexibility and allow automation where appropriate safeguards are in place.

The objective is to ensure consistency with:

- the principle of technological neutrality;
- the risk-based approach;
- operational efficiency; and
- the possibility of maintaining meaningful human intervention where necessary.

Amendment proposal:

EBF suggests amending Paragraph 78 to read: "Obligated entities that use automated or semi-automated mechanisms to support the investigation, assessment or closure of monitoring outputs should ensure that such mechanisms are underpinned by a documented and explainable decision logic, proportionate safeguards, and effective human oversight, calibrated to the level of risk associated with the case, including cases relating to higher-risk customers or situations requiring enhanced scrutiny. The use of automated or semi-automated mechanisms for such purposes should not, in itself, be excluded on the sole basis of the customer's risk classification, provided that appropriate safeguards are in place, including risk-based sampling, override and escalation capability, and periodic human validation of outcomes."

Comment 18: Paragraph 85 and 86

Rationale

Material changes to monitoring logic or methods can significantly affect detection effectiveness, alert volumes and operational capacity, especially where data inputs, segmentation, thresholds or scenarios change. To avoid inconsistent interpretations and ensure expectations are workable across different business models, the guideline should explicitly frame transition/validation as risk-based and proportionate and specify the core elements that should be documented (scope, rationale, governance/approvals, assumptions, data impacts, testing approach, limitations and remediation).

Paragraph 85 requires obliged entities to implement a validation framework to assess changes to monitoring or analytical approaches and further provides that such validation should include *"testing that goes beyond comparison with legacy outputs."* It is unclear what additional forms of testing AMLA expects obliged entities to undertake, or why comparison with legacy outputs would not, in itself, constitute an appropriate validation method. AMLA should clarify the intended scope of this requirement.

Amendment proposals

AMLA should either i) reformulate to clarify what is intended with the statement 'testing that goes beyond comparison with legacy outputs', and/or ii) specify what other kinds of testing may be required.

We propose the following amendment: "Where obliged entities materially change their monitoring logic, analytical methods or monitoring approach, they should apply a documented, risk-based and proportionate transition and validation framework to assess

whether the revised approach remains effective and consistent with the defined effective outcomes and their business risk assessment. Validation should include testing that goes beyond comparison with legacy outputs. Comparative analysis with prior approaches may be used where it provides meaningful insight into potential gaps or ML/TF risks.”

As for Paragraph 86, in order to not be bound to fixed time frames, as stated before, EBF would suggest replacing “without undue delay” with “in a timely, risk-based and proportionate manner, taking into account the nature, materiality and urgency of the issue identified, the complexity of the monitoring tool or model, and the remediation required.”

Comment 19: Paragraph 87

Rationale

The current wording of Paragraph 87 appears to imply that obliged entities should systematically assess whether the use of innovative tools or technologies would improve the effectiveness of their monitoring framework. While technological innovation can contribute to more effective AML/CFT controls, the decision to assess, adopt or deploy such tools should remain within the discretion of each obliged entity.

Introducing an expectation to conduct a prior assessment of innovative technologies could create an additional compliance burden and may be interpreted as an implicit obligation to consider or justify the non-use of such technologies. This would go beyond the principle of technological neutrality and would be disproportionate, especially where existing monitoring arrangements are already effective and commensurate with the entity’s risk profile.

Paragraph 87 should clarify that advanced analytical tools are not expected as a standard component of an effective monitoring framework. In line with the risk-based approach, obliged entities should determine the appropriate combination of manual, semi-automated and automated controls based on their ML/TF risk profile, business model, available information and operational needs.

Amendment proposal

EBF suggests amending Paragraph 87 as follows: “Obliged entities may consider whether the use of innovative tools or technologies could enhance the effectiveness of their monitoring arrangements. The decision to assess, adopt or deploy such tools or technologies should remain at the discretion of the obliged entity and should not be interpreted as creating an obligation to evaluate or implement innovative technologies.”

Comment 20: Paragraph 89

Rationale

Paragraph 89 does not clearly explain the relationship between the second and third sentences. We understand the second sentence as establishing a general obligation for obliged entities to implement appropriate safeguards when using advanced analytical tools, while the third sentence is intended to provide non-exhaustive examples of

safeguards that may be appropriate depending on the tool's nature, complexity, purpose, level of automation and impact on decision-making. The current wording could, however, be interpreted as requiring all of the listed safeguards in every case, which may be disproportionate and inconsistent with a risk-based approach.

Amendment Proposal

AMLA should clarify the interaction between sentence 2 and sentence 3.

EBF suggests revising wording in Paragraph 89 to clarify that the safeguards listed in the third sentence are illustrative rather than cumulative and should be applied as appropriate based on the nature, complexity, purpose, level of automation and impact of the advanced analytical tool concerned.

Question 5: Do you consider that the provisions on the use of automated or advanced analytical tools are sufficiently flexible and do not favour specific technologies?

If you see scope for further clarification, please:

(i) specify the paragraph concerned;

(ii) explain your rationale; and

(iii) consider submitting an amendment proposal

Limit: 3,000 characters for rationale, additional 3,000 characters for amendment proposals (optional) (max 10 comments)

The draft is broadly technology-neutral: it recognises manual, semi-automated and automated processes, does not make advanced analytical tools mandatory, and links safeguards to the role of the tool and the associated ML/TF risk. We welcome, in particular, the clarification in Paragraph 90 that explainability does not require full technical interpretability of the underlying model.

Further clarification would nevertheless be helpful to ensure that the requirements remain outcome-focused, proportionate and neutral between internally developed, vendor-provided, rule-based and advanced analytical tools.

Comment 1: Paragraphs 78 and 79: automated decisions and human oversight

Rationale

Paragraph 78 limits automated closure to cases that, following automated analysis, show no suspicious or unusual activity or material risk, and excludes higher risk customers.

The reference to “higher-risk customers” could be understood as a blanket prohibition on automated closure for all outputs relating to such customers. A higher customer risk classification should require enhanced scrutiny, but should not alone preclude automated

closure where the specific output has been assessed against reliable, current and verified information and does not reveal a material ML/TF risk indicator. Customer risk classification alone should not determine whether a specific monitoring output may be resolved through automation. A monitoring output relating to a higher-risk customer may nevertheless be a duplicate, a previously explained pattern or an output for which the relevant closure criteria can be reliably and consistently validated.

A blanket exclusion could generate unnecessary manual reviews of clearly non-suspicious outputs, divert resources from relevant cases and reduce the ability of obliged entities to deploy controlled automation in alert triage and investigation processes. It could also require the manual review of large volumes of outputs without necessarily improving the identification or escalation of genuinely suspicious activity.

Similarly, effective human oversight under Paragraph 79 should be understood as a proportionate governance and control framework. It should not necessarily require a human to review each individual automated decision where the mechanism is documented, validated, monitored and subject to appropriate exception and escalation controls. We suggest clarifying that for the purposes of these Guidelines, effective human oversight means that a natural person retains the ability to review, challenge, override or validate the outputs and does not require systematic case-by-case human review of every automated output or decision.

Risk-based automated and bulk closure of low risk alerts – with documented validation and sampling-based compliance monitoring – is essential to manage alert volumes and constitutes part of an effective and proportionate transaction monitoring system. We ask AMLA to confirm that this practice is allowed under Paragraphs 78-79, and that Paragraph 78 does not prevent the automated closure of alerts (also for higher risk customers) that, once analysed, are found to fall within the bank's risk appetite.

Moreover AMLA shall clarify the starting point of the delay from which the monitoring outputs are assessed (e.g., operation date, alert date).

Amendment proposals

- Confirm in Paragraph 78 that obliged entities may close alerts automatically across all risk categories where, following analysis, the closure is documented, validated and risk-based, and that a calibrated automated closure counts as a documented risk-based decision. EBF proposes amending Paragraph 78 as follows : “Automated or rules-based closure may be applied to defined categories of monitoring outputs where the available information does not indicate unresolved suspicious or unusual activity or other material ML/TF risk indicators. This may include outputs relating to higher-risk customers provided the closure criteria are documented and validated, subject to periodic sampling or quality assurance, and provided such mechanisms do not prevent the escalation of genuinely suspicious or unusual activity.”
- Avoid conflating “low risk alerts” with “low risk customers”: these are different concepts.
- EBF proposes adding the following clarification to Paragraph 79: “Effective human oversight may include governance approval, documented and understandable decision logic, periodic validation, sampling, quality assurance, performance monitoring,

exception management and escalation. It should not necessarily require manual review of each individual automated decision where the mechanism is validated and subject to appropriate controls.”

Comment 2: Paragraphs 87 – 95

Rationale

Paragraphs 87–95 address, in particular, issues relating to data protection. Further guidance would be helpful on the use of technology in compliance with data protection regulations. In addition, should the Guidelines envisage the use of artificial intelligence, such a requirement cannot be introduced through the Guidelines alone. It would require an appropriate legal basis in Level 1 legislation.

Amendment Proposal

EBF suggests amending Paragraphs 87–95 to provide additional guidance on the use of technology in compliance with applicable data protection requirements.

Comment 3: Paragraph 91: Reliance on third-party/vendor tools

Paragraph 91 restricts reliance on third-party tools where insufficient information is available. Banks commonly and legitimately rely on reputable third-party/vendor monitoring tools.

Paragraph 91 should clarify what constitutes “sufficient information” from a third-party provider. Without this clarification, the provision may unintentionally favour internally developed tools or providers able to disclose proprietary technical details. The information requirement should be proportionate to the tool’s role and materiality, and should enable the obliged entity to understand, govern, validate and challenge the tool’s outputs without requiring access to source code, model weights or other protected intellectual property.

Accordingly, we ask that Paragraph 91 not be read to effectively bar reliance on such tools where the entity applies proportionate governance, validation and oversight, and that “sufficient information” is interpreted at the level needed for effective oversight rather than full disclosure of proprietary vendor models.

Amendment proposal

AMLA should clarify in Paragraph 91 that proportionate assurance on third-party tools (validation, testing, oversight) suffices, without requiring full disclosure of vendor models.

We suggest amending Paragraph 91 as follows: “Where obliged entities rely on third-party providers, they should ensure that sufficient information is available, commensurate with the role of the tool and its impact on monitoring outcomes or decisions, to meet the requirements set out above. Such information should enable the obliged entity to understand the intended use, material limitations, governance arrangements, performance and outputs of the tool, and to review and challenge those outputs where necessary; it should not require disclosure of proprietary technical information or full technical interpretability of the underlying model. Where this is not the case, obliged

entities should not rely on such tools for monitoring functions that materially influence monitoring outcomes or decisions”.

Question 6a: What impact would the design and implementation of the transaction and activity monitoring framework described in Guideline 2 have on your compliance costs?

One option has to be chosen below:

- ☐ Increase of compliance costs and operational processes
- ☐ Reduction of compliance costs and operational processes
- ☐ No effect

Sub question 6a*: Increase/Reduction

One option has to be chosen below:

- ☐ Below 25%
- ☐ 50-75%
- ☐ More than 75%

Sub question 6a: Please explain the basis for your assessment, including the methodology used and any supporting evidence:**

N/A

Question 6b: Please rate the expected impact (very positive; positive; neutral; negative; very negative) on the following operational processes:

	Very positive	Positive	Neutral	Negative	Very negative
processes and controls;	☐	☐	☐	☐	☐
implications for staff;	☐	☐	☐	☐	☐
other (please specify)	☐	☐	☐	☐	☐

Other (please specify below):

Sub question 6b*: If you selected “negative” or “very negative” for any of the above under 3(b), please explain the basis for your assessment, including the methodology used and any supporting evidence, and indicate the distinction between one-off investment costs and recurring costs.

N/A

Question 7: Do you identify any further opportunities for simplification or measures that could further support proportionality across the guidelines?

(i) If so, please provide concrete drafting proposals and explain why the specific measures you propose would be more appropriate.

Limit: 5,000 characters

We encourage AMLA, in line with the principles of proportionality, technological neutrality and the risk-based approach in the “Background and rationale” section (sub-section 3.2), to ensure these Guidelines focus on the objectives and outcomes that Obligated Entities (OEs) should achieve through monitoring, rather than prescribing specific implementation models, methodologies or parameterisation requirements.

This would allow OEs to calibrate the intensity and design of their monitoring frameworks according to their ML/TF risk exposure and business profile, while maintaining flexibility regarding governance, operating models and technology. It would also ensure supervisory assessments focus on control effectiveness and risk mitigation outcomes, rather than particular organisational, operational or technological choices.

The Guidelines should continue to support technology-enabled innovation, including AI, advanced analytics and automation, while ensuring governance and oversight expectations remain proportionate to the role, materiality and risk profile of such tools. Implementation expectations should also take into account dependencies on external market infrastructure, including digital identity solutions, public registries and data availability, recognising that OEs should not be disadvantaged where relevant information is not reasonably accessible.

While these measures take the form of Guidelines rather than RTS or ITS, any resulting remediation would require an appropriate implementation period. Based on the sector’s experience, implementation would require a minimum transition period of 18 months following publication in the Official Journal. Should ex-ante monitoring remain a key expectation, an even longer implementation period may be necessary. More fundamentally, given the nature of banking activities and AML/CFT investigations, a framework based predominantly on ex-ante detection would not be operationally feasible. Proportionate, risk-based measures and an adequate implementation period are therefore essential for safe, effective and compliant implementation, taking due account of

operational realities and supporting consistent and harmonised application across the sector.

The most effective simplification would be to confirm that the periodic review in Paragraph 19 can be satisfied through perpetual KYC, i.e. continuous and trigger-based monitoring instead of a separate, time-scheduled review. As explained in our answer to Question 2, time-scheduled reviews largely duplicate what continuous monitoring achieves and lead to customer outreach with little added value. Meeting the periodic review obligation through monitoring outputs would significantly reduce costs and operational burden while maintaining or improving effectiveness. Paragraphs 19–20 should therefore clarify that the periodic review obligation may be satisfied by documented outputs of continuous and trigger-based monitoring, where reliable and independent sources are available, with customer contact only where a risk-relevant trigger arises.

It remains unclear how these Guidelines will interact with existing EBA/EC instruments, including which requirements will continue to apply and which will be repealed or superseded once the AMLA Guidelines take effect. This should be clarified to avoid overlap, duplicative work and conflicting interpretations by OEs and supervisors. AMLA should state explicitly which existing EBA Guidelines, or parts thereof, will be repealed or superseded and how any remaining EBA guidance interacts with these Guidelines.

EBF supports the horizontal nature of the Guidelines but considers that further clarification is needed for proportionate application across financial and non-financial OEs. OEs that do not execute or control transactions, have non-continuous business relationships, or have structurally limited access to transaction and activity data should be permitted to organise their monitoring around their actual role, business model, available data and relevant points of intervention.

Effective alternatives may include risk-based customer due diligence, assessment of instructions, mandates, contractual arrangements or assets, event-driven controls, staff escalation and post-activity review. The Guidelines should not require a banking-style continuous, real-time or automated transaction-monitoring architecture where this is not relevant to the entity's activities. Implementation should be proportionate to the OE's role, business model, scale, risk exposure, risk appetite, access to transaction and activity data and actual ability to assess or intervene. Documented structural limitations should not in themselves be treated as deficiencies where proportionate alternative controls enable effective identification and escalation of material ML/TF risks.