Consultation Response

Ongoing Monitoring - Consultation Response on draft Guidelines under Article 26(5)

Submission date: 3 September

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to comment on the AMLA Consultation on the draft Guidelines prepared as per the mandate given by Article 26(5) of Regulation (EU) 2024/1624. The Association for Financial Markets in Europe (AFME) is the voice of the leading banks in Europe's financial markets, providing expertise across a broad range of regulatory and capital markets issues. We represent over 150 leading global and European banks and other significant market players. Our members play a vital role in Europe's financial ecosystem, underwriting around 90% of European corporate and sovereign debt, and 85% of European listed equity capital issuances. Importantly, AFME members are market makers, providing liquidity, which is essential for ensuring financial markets can function efficiently. We also represent law firms and other associate members which advise market participants and support AFME's legal and regulatory initiatives.

AFME is registered on the EU Transparency Register, registration number 65110063986-76. We summarise below our high-level response to the consultation, which is followed by answers to the individual questions raised.

General commentary

AFME welcomes AMLA's efforts to promote a consistent and effective approach to ongoing monitoring. We support the overall objective of ensuring that obliged entities maintain an accurate and up-to-date understanding of their customers and are able to identify unusual or suspicious transactions and activities through effective ongoing monitoring.

AFME particularly welcomes the recognition in several areas of the draft Guidelines of the importance of adopting a risk-based, proportionate and technology-neutral approach. Several aspects of the draft Guidelines would benefit from further clarification to ensure consistent implementation and alignment with the AMLR framework.

In particular:

- The Guidelines should consistently reinforce that customer information updates, monitoring activities and follow-up actions are driven by material changes relevant to ML/TF risk, rather than formal or immaterial changes that do not affect an obliged entity's understanding of the customer or its ability to conduct effective ongoing monitoring.
- The Guidelines should avoid creating expectations that periodic reviews require comprehensive refresh exercises or the reassessment of all customer information in every instance. Obliged entities should retain discretion to determine, on a risk-based basis, which information remains relevant, reliable and sufficiently up to date.
- The Guidelines should maintain a clear distinction between periodic customer reviews under Article 26(2) AMLR and trigger-based reviews under Article 26(3) AMLR to avoid overlap, duplication and inconsistent implementation.
- The Guidelines should remain technologically neutral and sufficiently flexible to accommodate evolving approaches to customer information maintenance and monitoring, including the use of automated monitoring, reliable external data sources, advanced analytical tools and automated recertification processes where appropriate safeguards are in place.

Association for Financial Markets in Europe
London Office: Level 10, 20 Churchill Place, London E14 5HJ, United Kingdom T: +44 (0)20 3828 2700
Brussels Office: Rue de la Loi 82, 1040 Brussels, Belgium T: +32 (0)2 883 5540
Frankfurt Office: c/o SPACES – Regus, First Floor Reception, Große Gallusstraße 16-18, 60312, Frankfurt am Main, Germany T:+ 49 (0)69 710 456 660
www.afme.eu

Company Registration No: 6996678 Registered Office: Level 10, 20 Churchill Place, London E14 5HJ
AFME is registered on the EU Transparency Register, registration number 65110063986-76

- AMLA should seek to avoid duplication or overlap with obligations already addressed in the AMLR or in other AMLA mandates and technical standards. Where requirements are addressed in dedicated RTSs or other AMLA instruments, the Guidelines should signpost to those provisions rather than introducing potentially divergent expectations.
- The use of customer, group-level and external information should remain risk-based, proportionate and subject to applicable legal constraints, including data protection and confidentiality requirements.
- Given the significant interdependencies between these Guidelines and other AMLA measures that are not yet finalised, firms will require sufficient time to assess, implement and operationalise final requirements in a consistent and controlled manner.
- AFME notes that the Guidelines do not currently provide sufficient clarity regarding the timeframes within which monitoring outputs should be reviewed, investigated and resolved. In the absence of further guidance, competent authorities may adopt differing interpretations of what constitutes a timely resolution, creating inconsistent supervisory expectations across jurisdictions and increasing implementation complexity for cross-border institutions.
- AFME notes that the Guidelines do not provide sufficient clarity regarding the factors that competent authorities should take into account when assessing whether transaction monitoring outputs have been reviewed, investigated and resolved within an appropriate timeframe. AFME recommends that AMLA provide further clarification on the factors and supervisory principles that competent authorities should take into account. Any considerations provided should not be mandatory prescriptive measures and recognise that assessment and resolution timeframes will appropriately vary according to the complexity, materiality and ML/TF risk of a case. Early engagement with the private sector would be important to ensure that any resulting expectations are risk-based, operationally feasible and capable of consistent consideration across obliged entities.

AFME consultation responses

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? (20 comments)

If you see scope for further clarification, please:
(i)specify the paragraph concerned;
(ii)explain your rationale; and
(iii)consider submitting an amendment proposal

(i)specify the paragraph concerned;	**AFME amendments to AMLA paragraphs**	**(ii)explain your rationale; and**	**(iii)consider submitting an amendment proposal**
2	Article 26(2) of AMLR sets the maximum periods of time for updating customer information for both higher-risk customers and all the other customers. However, obliged entities should decide whether more frequent updates are needed based on the customer's risk profile. **If either a periodic or trigger-based** review is carried out earlier than scheduled, this can reset the timeline for the next	Paragraph 2 states that '*a review'* may reset the timeline for the next required update, but it is unclear whether AMLA intends this to apply only to comprehensive periodic reviews or also to more targeted event-driven reviews. Clarification is important because event-driven reviews are often narrower in scope and focused on a specific change,	AFME propose adding '*either a periodic or trigger-based' to replace 'a review'* and also adding *'where the scope and outcome of the review are sufficient to maintain an accurate and up-to-date understanding of the customer and associated ML/TF risks, taking into account materiality and the*

	required update **where the scope and outcome of the review are sufficient to maintain an accurate and up-to-date understanding of the customer and associated ML/TF risks, taking into account materiality and the risk-based approach.**	circumstance or risk indicator. When conducting periodic or event-driven reviews in accordance with Article 26(2) and Article 26(3) AMLR, the extent of any review, including whether review timelines should be reset, should depend on the materiality of any changes identified and their impact on the customer's ML/TF risk profile. The detailed application of these principles should be determined through the obliged entity's policies and procedures.	*risk-based approach'* to the end of paragraph 2.
3	When conducting periodic or event-driven reviews in accordance with Article 26 (2) AMLR and (3) of AMLR, obliged entities should assess ~~which elements of the customer information, including the customer risk classification, require updating. In doing so, they should take into account the customer's risk profile and the information already available to them, including how up to date that information is~~ **which documents, data or information are material for maintaining an accurate understanding of the customer and associated risks, including the customer's business activity and risk profile. The review should not require a full refresh of all customer due diligence information where existing information is considered by the obliged entity to remain sufficient, no material risk-relevant change has occurred, and the obliged entity remains able to conduct ongoing monitoring effectively.** Where the customer's risk has increased, obliged entities should apply appropriate risk-mitigating measures, **including obtaining additional information, where necessary, applying enhanced measures where the risk is higher** ~~obtain any additional information necessary to apply appropriate risk-mitigating measures, including enhanced measures where the risk is higher.~~	Guideline 1 is broadly supportive of a risk-based approach, but the current wording in paragraph 3 should be further clarified to avoid broad, automatic or formalistic refreshes of customer documents, data or information and to encourage effectiveness. Customer information reviews should focus on information that is material for maintaining an accurate understanding of the customer, the purpose and nature of the business relationship, the customer risk profile and the ability to conduct effective ongoing monitoring. The final Guidelines should clearly distinguish between material information gaps that affect CDD, risk assessment or monitoring, and purely formal or non-material data gaps that do not impair the obliged entity's ability to manage ML/TF risk. Additionally, additional information may not be required in all situations (e.g., where CDD rather than SDD is applied to low-risk customers that change to medium risk). The current drafting could result in a compliance exercise where obliged entities need to explain to supervisors why additional information has not been obtained.	Following AMLA's wording of '*obliged entities should assess …….'* we propose the addition of '*which documents, data or information are material for maintaining an accurate understanding of the customer and associated risks, including the customer's business activity and risk profile. The review should not require a full refresh of all customer due diligence information where existing information is considered by the obliged entity to remain sufficient, no material risk-relevant change has occurred, and the obliged entity remains able to conduct ongoing monitoring effectively.'* to replace *'which elements of the customer information…'* Paragraph 3 requires OEs to '*apply appropriate risk-mitigating measures',* we propose that this sentence should be followed with *'including obtaining additional information, where necessary'* in the final sentence, then retaining the original language of '*applying enhanced measures where the risk is higher'* at the end to replace the existing final sentence.
4	Ongoing monitoring should not be limited to transaction monitoring but should also capture relevant activities, behaviours and events throughout the business relationship.	The terms '*activities'* and '*behaviours'* are not defined and could be interpreted very broadly. Without further clarification, obliged entities may reach inconsistent conclusions regarding the scope	After AMLA's original paragraph 4 sentence AFME propose to add the following paragraphs:

	Activities and behaviours refer to monitoring material customer-level circumstances such as changes to personal details, beneficial ownership, employment or business activities, source of funds and source of wealth that the obliged entity would reasonably expect to be privy to through the course of the business relationship. **The terms should be applied in a risk-based and proportionate manner and should not be interpreted as requiring obliged entities to monitor behaviour outside the business relationship, outside their role, or beyond monitoring of information reasonably available to them.** **Ongoing monitoring references to *'behaviour'* should be understood as observable conduct arising from customer interactions, including the manner in which the customer uses products and services, provides information, responds to customer due diligence requests, or otherwise engages with the obliged entity, where such information is reasonably available to the obliged entity through the conduct of the business relationship.** **Obliged entities should assess whether such changes or behaviours, individually or collectively, affect the customer's money laundering, terrorist financing or sanctions risk profile and whether additional due diligence, review or investigation is warranted.**	of monitoring expected under the Guidelines, potentially also leading to divergent supervisory expectations and implementation across jurisdictions. This risks creating expectations that extend beyond the risk-based approach established in Article 26 AMLR and could result in firms seeking information that is not necessary to maintain accurate and up-to-date customer information. AFME considers that any reference to customer '*activities*' and '*behaviours*' should be limited to activities and behaviours of the customer that are relevant to the business relationship with the obliged entity, and which are known, or reasonably available, to the obliged entity. Also, AFME requests that the use of '*activities*' aligns with the definition/ reference to activities in wider AMLA instruments.	*'Activities and behaviours refer to monitoring material customer-level circumstances such as changes to personal details, beneficial ownership, employment or business activities, source of funds and source of wealth that the obliged entity would reasonably expect to be privy to through the course of the business relationship.* *The terms should be applied in a risk-based and proportionate manner and should not be interpreted as requiring obliged entities to monitor behaviour outside the business relationship, outside their role, or beyond monitoring of information reasonably available to them.* *Ongoing monitoring references to 'behaviour' should be understood as observable conduct arising from customer interactions, including the manner in which the customer uses products and services, provides information, responds to customer due diligence requests, or otherwise engages with the obliged entity, where such information is reasonably available to the obliged entity through the conduct of the business relationship.* *Obliged entities should assess whether such changes or behaviours, individually or collectively, affect the customer's money laundering, terrorist financing or sanctions risk profile and whether additional due diligence, review or investigation is warranted.'* To avoid ambiguity, AFME propose that the reference to '*events*' in paragraph 3a can be removed from drafting as event

			driven review is already a concept outlined within the instrument in accordance with paragraph 27, AMLA can instead signpost to these provisions, clarifying that it refers solely to trigger events relevant to the business relationship and customer risk profile.
19	Periodic reviews must always be conducted in accordance with Article 26(2) of AMLR. However, the depth and intensity of such reviews should follow a risk-based approach, whereby the obliged entity assesses, based on the customer's risk profile **and the nature of the business relationship**, which information, data, or documents require updating. **A periodic review does not necessarily require the simultaneous reassessment or updating of all customer documents, data and information depending on the risk profile and materiality.**	*General commentary* AFME supports the objective of ensuring that customer information remains accurate and up to date throughout the business relationship and recognises that periodic reviews remain an important component of the Article 26 AMLR framework. AMLA should proactively continue to review and assess periodic review sections of the Guidelines to ensure the regulatory approach is sufficiently flexible and technologically-neutral to accommodate evolving approaches to customer-information maintenance. Increasingly, some obliged entities are already making use of automated monitoring capabilities, reliable external data sources and risk-based controls that enable customer information to be assessed on an ongoing basis rather than primarily through traditional periodic-review processes. *Which information to update* Obliged entities should be able to determine which information remains relevant, reliable and sufficiently up to date when updating a periodic review and focus review activity on information that is material to maintaining an accurate understanding of the customer and associated ML/TF risks. Clarifying this point would reduce the risk that periodic reviews are interpreted as requiring comprehensive refresh exercises and would better align Paragraph 19 with the principles already	*Which information to update* AFME request that clarification is added to paragraph 19 with the following line at the end of the paragraph '*a periodic review does not necessarily require the simultaneous reassessment or updating of all customer documents, data and information'* . *Business relationship calibration* AFME recommend adding *'and the nature of the business relationship'* following *'.....*whereby the obliged entity assesses, based on the customer's risk profile'.

		reflected elsewhere in the Guidelines regarding proportionality, materiality and efficient ongoing monitoring. *Business relationship calibration* Additionally, paragraph 19 could provide greater clarity that the scope of a periodic review should be calibrated to the risks associated with the specific business relationship.	
20	One of the considerations in adjusting the depth and intensity of a periodic review is when a business relationship exists but no new activity has occurred since the last customer information update, and no new services or products have been offered to the customer **.** Where, in a business relationship, the same **activity in line with expectations and known patterns** continues ~~without any change~~, obliged entities may, **on a risk-based approach, adjust the depth and intensity of periodic reviews,** ~~for~~ **justified by the customer's risk profile and the absence of material change** ~~low-risk customers~~ **A periodic review may be completed without contacting the customer where the** ~~o~~**bliged** ~~entity can demonstrate that~~ **information obtained remains sufficient, accurate and appropriate for the risk profile**. ~~for low-risk customers for example, such review could mean checking business registries and other reliable and independent sources, conduct PEP and adverse media screening, and review internally whether anything has changed in the nature or purpose of the business relationship.~~ **Obliged entities should consider, amongst others, the following non-exhaustive list of factors when deciding whether and how to adjust the depth and intensity of a periodic review:** a) The customer's risk level b) ~~Whether new activity or transaction has occurred or new services / products have been offered to the customer~~ c) The type and risk level of products or services provided to the customer and	*Methods for conducting a periodic review* A periodic review should be capable of being satisfied through an automated recertification process where this is justified by the risk profile, and the obliged entity remains able to demonstrate that it has assessed whether customer information remains accurate, up to date and appropriate. This also support AMLA's objectives of technology neutrality and ensures the methodology for conducting periodic review is not constrained. *Refresh without customer outreach* Periodic review may be in various methods, including without customer outreach. Additionally, the text should focus on this occurring where the risk profile remains appropriate rather than limiting this only to low risk. *Trigger events impacting intensity* Paragraph 20 concerns the calibration of a periodic review under Article 26(2) AMLR and is distinct from the trigger-based review framework under Article 26(3) AMLR. AFME agrees that circumstances similar to those listed in paragraph 27 may be relevant when determining the appropriate depth and intensity of a periodic review. While such circumstances would ordinarily be relevant in the context of an event-driven review, they may also be identified during the course of a periodic review and, where this occurs, may justify a more extensive assessment of the customer information held. The AFME proposal focuses on the	*Methods for conducting a periodic review* AFME have proposed the addition of '*The periodic review referred to in Article 26(2) AMLR may be conducted through an automated recertification process where justified by the risk profile. This approach applies horizontally to all categories of obliged entities referred to in Article 3 of the AMLR, irrespective of sector, and is without prejudice to the obligation to conduct an event-driven review under Article 26(3) of the AMLR where a triggering event occurs.*' as a conclusion to the paragraph. *Refresh without customer outreach* The addition of *'A periodic review may be completed without contacting the customer where the obliged entity can demonstrate that information obtained remains sufficient, accurate and appropriate for the risk profile.*' has been proposed to replace *'...for low-risk customers. For example, such review could mean checking business registries and other reliable and independent sources, conduct PEP and adverse media screening, and review internally whether anything has changed in the nature or purpose of the business relationship'.* *Trigger events impacting intensity*

	whether, despite the absence of new activity, the risk profile does not justify reducing the depth and intensity of monitoring. ~~d) Whether a trigger event has occurred; where this is the case, a customer information review should be initiated without delay.~~ **e)** ~~Whether a new activity or transaction is initiated by the customer or by third parties; in such cases, a review should be carried out without delay.~~ ; **Whether information obtained during the periodic review suggests changes in customer circumstances (such as factors listed in paragraph 27) that may warrant a more intense assessment of the customer information held.** **The periodic review referred to in Article 26(2) AMLR may be conducted through an automated recertification process where justified by the risk profile. This approach applies horizontally to all categories of obliged entities referred to in Article 3 of the AMLR, irrespective of sector, and is without prejudice to the obligation to conduct an event-driven review under Article 26(3) of the AMLR where a triggering event occurs.**	information identified during the review rather than the occurrence of a trigger event itself, thereby avoiding any potential conflation between periodic reviews and event-driven reviews.	AFME has therefore proposed **removing bullet points b), d) and e)** to consolidate a number of overlapping factors and propose a drafting addition of '*Whether information obtained during the periodic review suggests changes in customer circumstances (such as factors listed in paragraph 27) that may warrant a more intense assessment of the customer information held.*' that focuses on the information identified during the review rather than the occurrence of a trigger event itself, thereby avoiding any potential conflation between periodic reviews and event-driven reviews.
21	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. Obliged entities should determine the appropriate scope of updates, taking into account the customer's overall risk profile **and considering the list below, setting out a non-exhaustive range of customer information:** ~~The list below sets out a non-exhaustive range of key customer information that needs to be assessed for the purpose of an update:~~	AFME agree 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. Obliged 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.	AFME propose to replace AMLA's existing language of '*The list below sets out a non-exhaustive range of key customer information that needs to be assessed for the purpose of an update'* and instead include '*and considering the list below, setting out a non-exhaustive range of customer information'*.

	a) The identification information on the customer, including the natural person or the beneficial owner in case of a legal entity; b) Beneficial ownership information, the legal status and valid statutory representation of legal entities; c) An up-to-date understanding of the purpose and intended nature of the business relationship including, where applicable, a clear understanding of the source of funds; and d) Whether the customer, beneficial owner of the customer and, where relevant, the person on whose behalf or for the benefit of whom a transaction or activity is being carried out has become a politically exposed person, a family member or person known to be a close associate.		
27	The following non-exhaustive list of events are provided as instances of what may trigger a review of customer information based on changes in the relevant circumstances of the customer or facts which pertain to the customer, pursuant to Article 26(3) AMLR. Obliged entities should update the customer information accordingly and, adopting a risk-based approach, assess whether any of the triggering events listed below constitute a relevant and material change to their customer's risk profile that would warrant a re-assessment and change of the customer's risk profile level. Such triggering events may include: a) Changes in identity, legal status or ownership: including updates to identity details, nationality or residency, changes in legal form, ownership **and control structure pursuant to article 53,** ~~directors, authorised signatories or representatives.~~ **and the legal representative(s) (e.g., legal guardians) of a natural person customer; any natural person, other than an internal employee or senior manager of a legal person, authorised to act on behalf**	*Directors and control* The reference to directors should be removed, as changes in directors often reflect routine personnel movements and are not, in themselves, indicative of a change in ML/TF risk. By contrast, changes involving individuals who exercise sufficient control to qualify as beneficial owners are more material and may affect the entity's risk profile. *Authorised signatories or representatives* AFME considers the reference to '*authorised signatories or representatives*' in paragraph 27(a) overly broad and capable of capturing employees acting in the ordinary course of business. Consistent with the Persons Purporting to Act definition proposed in AFME's June 2025 response to the EBA's call for advice on new AMLA mandates, the trigger should instead be limited to: • legal representatives of natural person customers; and	*Directors and control* AFME propose the removal of directors. AFME propose to include '*and control structure pursuant to article 53.*' *Authorised signatories or representatives* The proposed language to be added to the end of paragraph 27a) is as follows: '*and the legal representative(s) (e.g., legal guardians) of a natural person customer; any natural person, other than an internal employee or senior manager of a legal person, authorised to act on behalf of a legal person customer pursuant to a contractual mandate (e.g. an agent), or any natural person authorised to act on behalf of legal person customers pursuant to a bilateral proxy agreement.*' *IP addresses* AFME suggests deleting the reference to '*repeated or unusual changes in IP*

	of a legal person customer pursuant to a contractual mandate (e.g. an agent), or any natural person authorised to act on behalf of legal person customers pursuant to a bilateral proxy agreement.' b) Behavioural, **or** activity-based-or transactional anomalies: unusual transaction patterns,-inconsistent behaviour, frequent and unexplained changes of professional service providers, ~~repeated or unusual changes in IP address or device location~~, where relevant, or any activity that deviates from the customer's profile or from the expected purpose and intended nature of the business relationship. Obliged entities should consider AMLA's Guidelines pursuant to Article 69(5) AMLR on indicators of suspicious activity or behaviours. c) **Material** risk-relevant information or adverse findings: new adverse media, new PEP status, legal proceedings related to potential ML/TF violations, regulatory notices, internal intelligence or warnings issued by competent authorities. d) **Material** 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, new products or services used by the customer, or engagement with higher-risk jurisdictions or counterparties.	• external natural persons formally authorised to act on behalf of legal person customers under a contractual mandate or bilateral proxy agreement. Internal employees should be excluded. This distinction is particularly important in wholesale banking, where operational staff frequently interact with customers but do not hold formal authority. Including such individuals would create a disproportionate identification and verification burden without corresponding ML/TF risk benefits. *IP addresses or device locations* IP addresses and device-location data may be relevant in some digital or retail business models but are neither universally available nor applicable across sectors. Their inclusion as trigger events could create an expectation that firms routinely collect and monitor such data, contrary to a risk-based and proportionate approach. Where relevant, such information is more appropriately considered within other risk management frameworks such as transaction monitoring, and fraud prevention. *Materiality* Paragraphs 27 c) and 27 d) should incorporate a materiality threshold to ensure that only changes relevant to the customer's ML/TF risk profile trigger a review. In particular, the mere use of a new product or service, as referenced in paragraph 27 d), should not automatically require an update of customer information. Consistent with our comments on paragraph 20 e), firms should be able to determine, on a risk-based basis, whether the new product or service materially affects the customer's ML/TF risk profile or the firm's understanding of the purpose	*address or device locations'* as per paragraph 27b) *Materiality* AFME recommends the word '*material'* is included at the front of each of the sentences in point c) and d) of paragraph 27. For point d) after the wording *'source of funds or wealth or business...'* AFME also propose adding '*activity that deviates from the customer's profile or from the expected purpose and intended nature of the business relationship'* AFME also propose removal of the phrase '*financial situation'* from d).

		and intended nature of the business relationship. This would avoid unnecessary, formalistic reviews and ensure resources remain focused on genuinely risk-relevant changes. AFME also recommends removing the reference to a customer's '*financial situation*' in paragraph 27 d), as the most relevant financial factors are already captured elsewhere in the list. Finally, paragraph 27 d) should clarify that changes in a customer's business activity may trigger a review where they are inconsistent with the obliged entity's understanding of the customer.	

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? **(20 comments)**

If you see scope for further clarification, please:
(i)specify the paragraph concerned;
(ii)explain your rationale; and
(iii)consider submitting an amendment proposal

(i)specify the paragraph concerned;	**AFME amendments to AMLA wording**	**(ii)explain your rationale; and**	**iii)consider submitting an amendment proposal**
7	N/A	While AFME supports the principles of training in paragraph 7 and governance (paragraph 8), the mandate in Article 26(5) is strictly on the monitoring of relationships and transactions. It does not explicitly grant a mandate to issue Guidelines on staff training (primary obligation in Art. 12 AMLR) or the extent of internal policies, procedures, and controls (primary mandate in Art. 9(4) AMLR). Including detailed rules here pre-empts or duplicates those mandates.	No amendment

8	Obliged entities should ensure that the governance of their ongoing monitoring framework, including the related decision-making processes, is documented in their internal policies, procedures and controls, in a manner that supports traceability, accountability and effective supervision. This should include documenting any material limitations **relevant to the ML/TF risks being mitigated** arising from the nature of their business, the mitigating measures applied to address those limitations, and the resulting monitoring outcomes. They should be able to understand what was assessed, what decisions are taken and the rationale behind. The form, level of detail and means of documentation should be proportionate to the ML/TF risk being mitigated and the nature, risks and complexity of their business, as well as the size of the obliged entity. **Where the obliged entity forms part of a group, the governance of the ongoing monitoring framework should clearly document the respective roles and responsibilities of the obliged entity and any group-level functions. Where group-wide policies, methodologies, tools or oversight are relied upon, the obliged entity should remain responsible for understanding, assessing and documenting the decisions taken, their rationale and their impact on its ML/TF risk exposure. The obliged entity should retain sufficient oversight and control to ensure that its ongoing monitoring framework remains appropriate to its specific business activities, risk profile and legal obligations.**	*Governance for group structures* AFME welcomes further clarification on how this governance expectation should apply in the context of group structures, particularly in the context of the group-wide requirements set out in Article 16 AMLR. As currently drafted, the paragraph appears to be framed solely from the perspective of a standalone obliged entity. In practice, some firms may operate within a group environment where policies, methodologies, tools or governance arrangements are developed and maintained at group level. The guidance should therefore recognise these operating models while making clear that ultimate accountability remains with the obliged entity. At the same time, it should avoid creating the impression that governance, risk assessment or decision-making must be fully centralised or delegated to a group function, particularly in the case of firms that are part of non-EU headquartered groups where responsibilities may be allocated differently. Where group-level policies, methodologies or oversight are relied upon, the obliged entity should be able to demonstrate how these have been considered and applied in the context of its own business, risks and legal obligations. This would better reflect the interaction between entity-level accountability and group-wide arrangements under Article 16 AMLR, including where parent undertakings or central functions are located outside the EU. *Qualifier* Relevance to the ML/TF risks being mitigated has been added to qualify documenting any material limitations to ensure limitations regarding governance are appropriately scoped.	*Governance for group structures* Suggested addition at the end of paragraph 8 of '*Where the obliged entity forms part of a group, the governance of the ongoing monitoring framework should clearly document the respective roles and responsibilities of the obliged entity and any group-level functions. Where group-wide policies, methodologies, tools or oversight are relied upon, the obliged entity should remain responsible for understanding, assessing and documenting the decisions taken, their rationale and their impact on its ML/TF risk exposure. The obliged entity should retain sufficient oversight and control to ensure that its ongoing monitoring framework remains appropriate to its specific business activities, risk profile and legal obligations.*'
12	Depending on the nature of the documents, data or information to be updated, and on the level and type of risk that needs to be mitigated, obliged entities should apply risk sensitive measures in line with the	**1..Remove paragraph 12 in its entirety** The requirements relating to customer information sources and updates are already addressed in the CDD RTS. Paragraph 12 overlaps with provisions in Article	AFME have proposed a primary proposal to remove paragraph 12 in its entirety. If paragraph 12 is not deleted for the

	RTS adopted pursuant to Article 28(1) of AMLR to assess the reliability and independence of the information source. Customer information should be updated by using: include, where relevant and appropriate, one or more of the following: a) Reliable and independent sources of information which may include official registers or databases of government and competent authorities b) Information collected through reliable and reputable commercial organisations such as vendors and data service providers, and information from reliable and independent open sources; c) Information or confirmation provided directly by the customer, either in writing or through digital means or directly through personal interaction with the obliged entity, provided that such information is appropriately documented by the obliged entity., provided that this information is of sufficient quality to enable them to assess the authenticity and accuracy of the information; d) Information provided by other obliged entities; e) Internal information and records held by the obliged entity in the course of the business relationship, including transaction and activity monitoring; f) A combination of the sources above.	28(1), Recital 5, Article 10 and Article 27 of the RTS, creating uncertainty as to whether the source lists in these Guidelines are intended to be exhaustive, supplementary or standalone. AFME therefore recommends deleting paragraph 12 and instead cross-referring to the relevant RTS provisions to ensure consistency across AMLA instruments and avoid duplication. **2. If paragraph 12 is retained** *General comment - Operational considerations* For ongoing monitoring, it is common industry practice for customers to confirm whether relevant changes have occurred rather than for firms to independently re-validate all customer information. Requiring further validation in all cases would be difficult to operationalise and is unlikely to be proportionate, particularly where firms have no practical means of independently verifying the information provided by customers. *Illustrative rather than prescriptive sources* While the opening sentence supports a risk-based approach, the subsequent reference to a specific list of sources could be interpreted as mandatory. AFME therefore requests clarification that the list is illustrative and non-exhaustive. To achieve this, AFME proposes adding the words: '*Include, where relevant and appropriate, one or more of the following'.* Recognition of customer-provided information Paragraph 12(c) should permit information obtained directly through customer interactions, provided that it is appropriately documented by the obliged entity. AFME also considers the current reference to information being of '*sufficient quality'* to be circular and potentially duplicative of the verification requirements in paragraph 14. The concept would be more appropriately addressed within paragraph 14,	aforementioned reasons, AFME proposes the following: Illustrative rather than prescriptive sources Adding the words '*include, where relevant and appropriate, one or more of the following'*. To replace '*be updated by using:*' Recognition of customer-provided information AFME proposes inserting: '*or directly through personal interaction with the obliged entity, provided that such information is appropriately documented by the obliged entity.*' to Paragraph 12(c) AFME also propose a deletion of '*provided that this information is of sufficient quality to enable them to assess the authenticity and accuracy of the information;'* AFME proposes adding *'internal information and records held by the obliged entity in the course of the business relationship, including transaction and activity monitoring.'*

		where customer-provided information that is not of sufficient quality would be subject to supplemental verification using reliable and independent sources. Use of existing information held by the obliged entity Internal records should be a recognised source of information.	
13	Obliged entities should take ~~necessary~~ **reasonable** steps to ensure ~~that personal data obtained from public and commercial sources is~~ **accurate and up to date~~,~~ the accurate and timely transfer of personal information into internal systems, using the latest version of information available to the obliged entity on an ongoing basis.'** ~~and that~~ **Obliged entities should also ensure** only the information necessary to fulfil their ongoing monitoring obligations is collected and processed **as determined by the obliged entity's own risk-based assessment. Where obliged entities rely on official registers or databases of governments or competent authorities referred to in paragraph 12(a), they should not be expected to independently verify or guarantee the accuracy, completeness or timeliness of the underlying source data, unless there are reasonable grounds to doubt the information obtained.**	We note that Paragraph 13 would benefit from clarification as to the extent of the obligation on obliged entities when relying on information obtained from public or commercial sources. Paragraph 13 should clarify that, where obliged entities rely on commercial registers or databases of governments and competent authorities as referred to in paragraph 12(a), they are not responsible for guaranteeing the underlying source data being '*accurate'* and '*up-to-date'*. AFME suggests amendments to the wording to reflect the context within which members can internally ensure that data obtained from such sources is up to date *Necessity of information to fulfil ongoing monitoring* Replacing a rigid necessity test with a risk-calibrated standard aligns this obligation with the principle of proportionality already embedded within the AML/CFT regulatory framework.	*Necessity of information to fulfil ongoing monitoring* Replace '*necessary'* steps with '*reasonable'* steps and add *'the accurate and timely transfer of personal information into internal systems, using the latest version of information available to the obliged entity on an ongoing basis.***'** to replace *'that personal data obtained from public and commercial sources is accurate and up to date'*. Following '*only the information necessary to fulfil their ongoing monitoring obligations is collected and processed'* adding '*as determined by the obliged entity's own risk-based assessment…***'** Addition of **'***Where obliged entities rely on official registers or databases of governments or competent authorities referred to in paragraph 12(a), they should not be expected to independently verify or guarantee the accuracy, completeness or timeliness of the underlying source data, unless there are reasonable grounds to doubt the information obtained.'* to the end of the paragraph.
14	With regards to paragraph 12, point c, where a customer provides ~~a written statement with~~ new information or confirms previously collected information, documents, or data, obliged entities should, depending on the level and nature of the risk, consider whether the reliability of that statement needs to be verified using independent and reliable	**Option 1: Rationale for proposed deletion of independent and reliable provisions** We refer to AFME's response to the CDD RTS regarding independent and reliable sources. Requirements concerning the reliability, accuracy and verification of	AFME requests consideration of the following options. **Independent and reliable provisions** **Option 1: AFME's primary proposal is to remove the reliability-related provisions in paragraph 14**

	sources. In cases where a person representing the customer, **provided they are not an employee of the customer**, provides the confirmation on behalf of the customer, obliged entities should assess if they have the necessary knowledge and power of representation to confirm or provide such information. **Where a person acting on behalf of the customer has already been verified as authorised to do so, obliged entities should be able to rely on existing records unless there are reasonable grounds to question that person's authority or ability to provide or confirm the relevant information.**	customer-provided data are covered under Art 33 of the AMLR and the CDD RTS. **Option 2: If paragraph 14 is retained, rationale for amendments** Provided that equivalent requirements are retained in the final CDD RTS. Alignment of the drafting with the CDD RTS would avoid duplication, promote consistency across the AML framework and ensure that detailed verification requirements remain within the appropriate legislative instrument and mandate. *Necessary knowledge and power of representation* The concepts of '*necessary knowledge'* and '*power of representation'* are not defined and could be interpreted inconsistently across obliged entities. AFME therefore requests that AMLA either provide illustrative examples of circumstances that would satisfy these requirements or clarify the objective criteria that obliged entities should consider when making this assessment. *Written statements* Customer information is frequently obtained, confirmed or updated through face-to-face interactions, telephone discussions or other established channels, not necessarily a written statement by the customer. The provision should therefore remain neutral as to the method through which information is obtained *Non-employees of the customer* AFME supports retaining the clarification regarding employees of the customer. Employees acting within their authorised functions may reasonably be expected to provide or confirm customer information as part of the ordinary course of business and should not automatically be subject to the same assessment regarding knowledge and power of representation as external representatives. *Existing authorisation verification*	**Option 2: If this is not deleted, AFME proposes the following:** AMLA should align the drafting with the final CDD RTS and clarify that reliability should be assessed using a risk-based approach, taking into account the nature of the information, the source from which it is obtained and the circumstances of the business relationship. This would reduce the risk of divergent interpretations and ensure consistent application of customer due diligence requirements across the EU. *Necessary knowledge and power of representation* AFME requests that AMLA either provide illustrative examples of circumstances that would satisfy these requirements or clarify the objective criteria that obliged entities should consider when making this assessment. *Written statements* AFME propose deleting '*a written statement with*' *Non-employees of the customer* AFME has requested the addition of *'provided they are not an employee of the customer' following 'In cases where a person representing the customer…*; *Existing authorisation verification* To the end of the paragraph adding: '*Where a person acting on behalf of the customer has already been verified as authorised to do so, obliged entities should be able to rely on existing records unless there are reasonable grounds to question that person's authority or ability to provide or confirm the relevant information*,

		Additionally, once a person's authority to act on behalf of a customer has been appropriately established and verified, obliged entities should be entitled to rely on existing records unless there are specific circumstances that call that authority into question. Requiring repeated reassessment of previously verified representatives would create unnecessary operational burden without a corresponding AML/CFT benefit. *Written statement* Finally, consistent with AFME's request under paragraph 12c) regarding recognising obtaining information based on face-to-face customer interaction as an acceptable source alongside written and digital means	*Written statement* AFME requests removal of '*a written statement with'* .
16	**Where identity documents or equivalent are used, obliged entities should establish and maintain risk-based policies and procedures that determine the circumstances in which expired identity documents, passports or equivalent documentation are required to be updated as part of customer information updates pursuant to Article 26(2) AMLR or event-triggered reviews under Article 26(3) AMLR.** ~~During the process to update customer information to comply with Article 26 (2) of AMLR or during an event trigger review according to Article 26 (3) of AMLR, obliged entities should assess whether expired identity documents, passports or equivalent should be updated, including for natural persons or beneficial owners in respect of a legal entity.~~ Where**, in accordance with those policies and procedures,** obliged entities conclude that an expired identity document, passport or equivalent should be re-collected **based on a relevant trigger event such as update to customer information**, ~~or where a new or additional beneficial owner/s of a legal entity or a new person purporting to act on behalf of the customer that needs to be identified and verified,~~ different methods of verification can be used such as	AFME supports a policy-based, risk-based approach to expired identification documents. Paragraph 16 should allow obliged entities to establish, through internal policies and procedures, the circumstances in which re-collection is necessary. In the absence of a material change in customer information or another relevant trigger event, obliged entities should not be required to reassess whether an expired document must be re-collected during each review. AFME would welcome slight adjustments to the wider text to consistently make clear that although this section refers to identity documents, passports or equivalent documents, the provision applies only where such documents are used by obliged entities rather than expressing a preference for identity documents in the context of beneficial ownership. As a result, AFME propose addition of wording at the beginning of the paragraph to outline that *'Where identity documents or equivalent are used….'* obliged entities should establish and maintain risk-based policies and procedures that determine the circumstances in which expired identity documents, passports or equivalent documentation are required to be updated as part of customer information updates	AFME propose addition of wording at the beginning of the paragraph to outline that *'Where identity documents or equivalent are used….'* *Policy-based approach to expired documents* *Re-collection where a material event occurs* AFME propose the addition of '*based on a relevant trigger event such as update to customer information'* Addition of '*in accordance with those policies and procedures*,' in between '*where…….obliged entities conclude…'* *Removal of redundant text* *'As per Article 22(6), point (b) and for beneficial owners Article 22(7) of AMLR'* has been removed.

	electronic identification means ~~as per Article 22(6), point (b) and for beneficial owners Article 22(7) of AMLR.~~	pursuant to Article 26(2) AMLR or event-triggered reviews under Article 26(3) AMLR. In addition, where a new or additional beneficial owner, or a person acting on behalf of a customer, is identified, this does not constitute '*re-collection of expired documents*'. AFME therefore considers that this wording would be more appropriately addressed within the Article 28(1) RTS provisions relating to the identification and verification of beneficial owners and persons acting on behalf of customers with appropriate signposting added to these Guidelines. This also corresponds with Article 28 which does not require the re-verification of beneficial ownership through identity documents; rather, it requires '*reasonable measures'* to be undertaken. *Policy-based approach to expired documents* AFME supports a policy-based, risk-based approach to expired identification documents. Paragraph 16 should allow obliged entities to establish, through internal policies and procedures, the circumstances in which re-collection is necessary, rather than requiring an ad hoc assessment during each review. *Re-collection where a material event occurs* Additionally, in the absence of a material change in customer information or another relevant trigger event, obliged entities should not be required to assess whether an expired document must be re-collected. *Removal of redundant text* *'As per Article 22(6), point (b) and for beneficial owners Article 22(7) of AMLR'* has been removed because Article 22(6), point (b), and Article 22(7) are specific to legal entities, whereas Article 22(6) is broader. Unless the intent is to exclude explicit reference to natural persons, this wording can be removed in line with AMLA's simplification objective.	

17	To assess whether or not to update an expired identity document, passport or equivalent, ~~obliged entities~~ **the policies and procedures outlined in Paragraph 16** consider, amongst other elements, the following factors ~~and the following~~ **as relevant:** a) The relevant risk associated with the customer and the business relationship that would call for an update of an expired identity document, passport or equivalent; b) ~~The risk associated with the issuing country~~; c) ~~The length of time that the identity document, passport or equivalent is expired~~; d) Whether it has all the necessary up-to-date security features **to the extent possible** since older identification documents might pose a heightened security risk of fraud and might be easier to counterfeit; ~~e) Whether a newly issued document would provide updated or additional information relevant to verifying the updated customer's identity or customer's risk assessment; and~~ f) Whether there are doubts as to continued accuracy of the customer's identification details, including doubts arising regarding the authenticity or adequacy of previously obtained identification data, or where such doubts may give rise to suspicions of ML/TF.	*Introductory text amended* '*Policies and procedures'* have been included as per rationale provided for 16. Rationale for removal of factors The factors in paragraph 17 should be limited to those that provide a meaningful indication that previously obtained identification information may no longer be accurate, reliable or sufficient. Several of the proposed factors (b, c and e) do not meet this threshold and risk generating unnecessary document refresh exercises without materially improving the effectiveness of customer due diligence. *Length of time expired* The length of time a document has been expired is not, in itself, a reliable indicator that a customer's identity information has changed or that the original identification is no longer valid. Requiring monitoring based on document expiry would create significant operational burdens and is not expressly required by the Level 1 text. A more proportionate approach would be to obtain updated documents where a relevant trigger event indicates that customer information may no longer be accurate or up to date. *Newly issued documents possibly providing updated or additional information* Regarding point e), Obliged entities are generally not in a position to determine proactively whether a newly issued document would contain additional or different information compared to a previously verified document. This assessment would require detailed knowledge of document formats and issuance practices across multiple jurisdictions and may therefore create expectations that are not operationally achievable. The focus should instead be on obtaining updated information where there is a relevant trigger event or indication that customer information may no longer be accurate.	AFME propose to replace '*obliged entities'* with '*the policies and procedures as outlined in Paragraph 16'*. AFME proposes amending the opening of paragraph 17 by replacing '*and the following'* with '*as relevant'*. AFME propose removal of b), c) and e). *Newly issued documents* The primary AFME drafting proposal is to remove point e), if this is not possible, we request this is qualified with the phrase '*where possible'*. *Security features* AFME proposes retaining point d) but adding the qualification '*to the extent possible'* after the reference to security features.

		High risk jurisdiction of identity document issue Regarding Paragraph 17 b) the principle of 'once identified, always identified' should apply regardless of the customer's jurisdiction. Country risk should inform the overall customer risk assessment rather than serve as a proxy for questioning the validity of identity documents that have already been obtained and verified. Automatically requiring re-collection solely because the issuing country is considered higher risk would not be consistent with a genuinely risk-based approach. The Guidelines should instead focus on specific facts or circumstances that raise doubts as to the authenticity or validity of the document. *Security features* This has been added as a qualifier to 'necessary security features' to demonstrate that this is undertaken on a best-efforts basis.	
18	When the ~~obliged entity~~ **policies and procedures outlined in Paragraph 16** deem it necessary to update an expired document, passport or equivalent**, these policies and procedures** should determine, based on the level of risk whether the expired document: a) needs to be ~~updated without delay;~~ **updated within a timeframe proportionate to the level of risk identified; or** b) the update takes place during the next scheduled customer information review or at the next occasion on which the customer interacts with the obliged entity, such as when requesting a new service or product.	*Policies and procedures* AFME is concerned that, paragraphs 16 and 17, paragraph 18 could be interpreted as requiring obliged entities to make, document and justify an individual case-by-case assessment each time an expired document is encountered. This would be inconsistent with a policy-based and risk-based approach and could create unnecessary operational burden without improving risk outcomes. In line with earlier comments, Paragraph 18 should therefore clarify that the timing of any update is determined through the application of those policies and procedures, rather than through a new ad hoc assessment in every case. *Undue delay* Additionally, the use of the phrase '*without delay*' in paragraph 18 a) introduces an ambiguity that risks inconsistent application across obliged entities. '*without delay*' may be interpreted by supervisory authorities as requiring immediate or near-immediate	*Policies and procedures* AFME propose to replace '*obliged entities'* with '*the policies and procedures*' *Undue delay* AFME propose adding **'***updated within a timeframe proportionate to the level of risk identified'* **t**o qualify the expectation.

		action, which in many cases would be operationally disproportionate and unreflective of the risk-based rationale that underpins the broader customer due diligence framework.	
30	Pursuant to Articles 20, 21 and 26 of AMLR, where an obliged entity is unable to keep the relevant customer documents, data or information up to date, it shall refrain from carrying out transactions and shall terminate the business relationship **unless there is contradiction with the local law**. Where an obliged entity needs to obtain updated documents, data or information from the customer, or to seek customer confirmation, and no response is received, and this temporarily prevents compliance with Article 20(1), point (f), of the AMLR, the obliged entity may, before terminating the business relationship, temporarily suspend or restrict transactions, activities or services. Such measures should be applied only where they allow the ML/TF risks to be effectively managed. When assessing whether it is appropriate and possible to suspend or restrict transactions, activities or services, obliged entities should take into account the following factors: a) No trigger event within the meaning of Article 26(3) has occurred; b) Considering the risk level of the customer; c) The nature of the products or services provided to the customer, and whether the suspension or restriction of transactions, activities or services is sufficient to effectively mitigate the ML/TF risks of the business relationship, thereby justifying a longer interval between updates; and d) The documents, data or information already available remain sufficient to manage the identified risks, taking into account the scope of the suspension or restriction applied.	The Guidelines mandate that if an obliged entity is ultimately unable to obtain updated CDD information, it must terminate the business relationship however, in several EU jurisdictions (such as France), unilateral contract termination by a financial institution is strictly restricted or prohibited under local consumer, insurance, or banking regulations. This creates an irreconcilable conflict where complying with the AMLA guidelines would place the institution in direct violation of national law. Following the existing line of '*and shall terminate the business relationship',* AFME has proposed the addition of '*unless there is contradiction with the local law*' AMLA should consider providing examples of how obliged entities to navigate these scenarios.	Following '*it shall refrain from carrying out transactions and shall terminate the business relationship…*' AFME propose adding *'unless there is contradiction with the local law.'*
32	Obliged entities should take all reasonable measures and make every effort to obtain and update such documents, data, or information as soon as possible. The suspension or restriction of transactions and	See rationale as per paragraph 31 commentary.	In line with AFME comments on paragraph 31 '*if this is in accordance with local laws and regulations*.' is to be added to the end of the paragraph .

	activities should be understood as a temporary measure, to be applied only where an obliged entity has taken repeated and reasonable steps to request and obtain up-to-date customer documents, data or information, and only until the obliged entity obtains the necessary documents, data or information from the customer. Termination should follow where the obliged entity is ultimately unable to comply with its obligations **if this is in accordance with local laws and regulations.**		

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:

- **Increase of compliance costs and operational processes - 25-50%**
- Reduction of compliance costs and operational processes
- No effect

Follow-on question
Please explain the basis for your assessment, including the methodology used and any supporting evidence

This assessment is based on feedback from AFME member firms regarding the expected operational, resource, technology and cost implications of implementing the proposed requirements, drawing on their internal consultations with regulatory change management teams and external due diligence vendors.

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				X	

	Very positive	Positive	Neutral	Negative	Very negative
event-driven reviews;				X	
implications for staff;				X	
other (please specify) **IT systems**					X

AFME Response
AFME assesses the impact of the proposed requirements as **negative** across customer review processes, staffing and, in particular, customer due diligence systems.
The Guidelines cross-reference multiple AMLA technical instruments that have not yet been published or finalised yet, meaning firms will require sufficient time to analyse, interpret and implement the final requirements. The measures are expected to necessitate significant changes to policies, procedures, customer review frameworks and supporting systems. Members anticipate implementation to be resource-intensive and costly, particularly given the compressed implementation timeframe.
The requirements are also likely to increase the frequency of customer record reviews, resulting in additional customer outreach, document collection and verification activities. This would increase operational workloads and require additional compliance and operational resources.

Current compliance costs are already substantial; therefore, even an increase at the lower end of this range would translate into a very significant amount. Members further anticipate significant technology and change-management costs. Existing customer lifecycle management and AML systems would need to be reviewed and adapted, often in consultation with internal technology and change teams as well as external service providers. Firms that rely on outsourced solutions or third-party vendors for customer due diligence processes expect implementation costs to increase further, as vendors will also need to update their systems and services within a limited timeframe. Given the anticipated market-wide demand for such changes, members expect increased pricing for vendor support and system enhancements.

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 **(20 comments)**

(i)specify the paragraph concerned;	**AFME amendments to AMLA paragraphs**	**(ii)explain your rationale; and**	**iii)consider submitting an amendment proposal**

34	Obliged entities should ensure that their monitoring framework, including transaction and activity monitoring processes and controls, is based on their business-wide risk assessment and: a) Leverages systems and processes required by other Union legislation, such as Regulation (EU) 2023/1113 ~~or the proposal on payment services in the internal market (PSR),~~ as well as other already existing systems intended to detect unusual customer behaviour. b) Relies on complete, accurate, and timely data, drawing on sources available internally, and, where relevant, reliable and independent sources, including group information exchanged pursuant to Article 16(3) of AMLR **on a risk-sensitive basis when it is proportionate and legally permissible to do so ;** c) Covers all products and **services relevant to the business relationship of the obliged entity**, **in a manner that is risk-based and proportionate**, in order to enable a holistic understanding of the customer's behaviour and support the detection of unusual or suspicious transactions and activities. d) Is capable of identifying transactions and activities that materially deviate from expected behaviour and may be unusual or suspicious, requiring further assessment under Article 69(2) AMLR; e) Is capable of identifying patterns, behaviours or linkages that may indicate risks related to the non-implementation or evasion of targeted financial sanctions, insofar as such risks are identifiable through the ongoing monitoring framework, including through intermediaries, ownership or control structures, counterparties, assets or transaction patterns; f) Is designed to be effective, at the point of implementation, in addressing the risks identified in the obliged entity's business-wide risk assessment, and to remain effective and fit for purpose over time through ongoing testing and adaptation to emerging risks.	AFME welcomes the provisions within paragraph 10 of Guideline 1 that appropriately recognise the need to balance effective monitoring with data protection requirements, including the principles of necessity and data minimisation under applicable data protection frameworks. We support this risk-based and proportionate approach; however, we note that paragraphs 34c) and 44 refer to developing a '*holistic understanding*' of customer activity across products and services. While we understand the supervisory objective underpinning this concept, AFME believes that the Guidelines should also qualify the mention of '*timely data.*' with the addition of '*on a risk-sensitive basis when it is proportionate and legally permissible to do so'* would be helpful to ensure consistency with the approach set out in paragraph 10. *Payment service regulations* AFME members cannot leverage systems and proposes that have not yet been finalised. This enables obliged entities to take into account the obliged entity's business model, products and services, operational role, data availability, and the nature of the ML/TF risks being monitored. AFME further recommends clarifying that the reference to information obtained from '*reliable and independent sources, including group information exchanged pursuant to Article 16(3) AMLR*' as per 34b) should be qualified as it should not be interpreted as requiring obliged entities to systematically obtain or use all potentially available group information for monitoring purposes. The use of group information should remain subject to relevance, reliability, legal permissibility, data availability, purpose limitation, confidentiality and operational feasibility. Obliged entities should be able to determine, on a risk-centred basis, which internal, external and group-level information is appropriate and proportionate to support effective monitoring in the specific circumstances. *Products and services* AFME propose to clarify that monitoring requirements only apply to the products and services offered by the specific obliged entity that has established the business relationship with the customer. AFME also propose adding '*This should only be subject to wider*	Payment service regulations AFME propose to delete '*or the proposal on payment services in the internal market (PSR),'* qualify the mention of '*timely data.*' with the addition of *'in a manner that is risk-based and proportionate'* AFME propose adding '*on a risk-sensitive basis when it is proportionate and legally permissible to do so ;*' to the end of the sentence. *Products and services* For point c), AFME recommends adding *'relevant to the business relationship of the obliged entity'* following '*….Covers all products and services'*

		information sharing within groups proportionate and legally permissible to do so in accordance with article 16(3).' AFME recommends clarifying that monitoring frameworks should primarily rely on information available to the obliged entity that has established the business relationship. The reference to group information exchanged pursuant to Article 16(3) AMLR should not be interpreted as requiring the systematic collection or aggregation of customer information from across a group, but rather as permitting the use of such information where relevant, proportionate and legally permissible.	
37	N/A	Further clarification would be helpful regarding the definition and intended scope of the term '*intermediary*' in this context. It should also be highlighted that obliged entities cannot provide feedback on the impact of this paragraph without AMLA's Guidelines on outsourcing being published	No amendment
38	N/A	Further clarification would be helpful regarding the definition and intended scope of the term '*intermediary*' in this context. It should also be highlighted that obliged entities cannot provide feedback on the impact of this paragraph without AMLA's Guidelines on outsourcing being published but AFME request AMLA to ensure consistency with the level 1 definitions.	No amendment
43	Obliged entities should ensure that their monitoring framework is capable of identifying and assessing ~~without undue delay~~ new ML/TF methods, trends and typologies **within a reasonable time frame** including those related to the non-implementation or evasion of targeted financial sanctions, identified by, amongst others, supervisory authorities, FIUs and other reliable public sources, as well as relevant risk indicators and red flags. They should assess and document whether there is a need to amend or supplement their monitoring framework. Obliged entities should revisit earlier decisions regarding their framework where needed, including as part of the review of their business-wide risk assessment and in response to internal cases, supervisory feedback or other credible external information and insights. They should be able to demonstrate to competent authorities	*'Undue delay'* could be interpreted as requiring immediate implementation of changes whenever new typologies, trends or risk indicators emerge. In practice, obliged entities require sufficient time to assess the relevance of such developments, complete appropriate governance and testing processes, and implement any necessary amendments in a controlled manner. AFME notes that paragraph 43 requires obliged entities to implement identified enhancements '*without undue delay*'. However, when read together with paragraph 49, obliged entities are also expected to assess the impact of changes, undertake testing and validation, document and record updates, and communicate changes to relevant staff. These activities are essential to ensuring that modifications do not inadvertently reduce detection capabilities or create unintended monitoring gaps but which cannot be concluded immediately.	AFME propose to replace '*without undue delay*' with '*within a reasonable time frame*'.

	the steps taken, the rationale for their decisions and the timing of their actions.		
44	Obliged 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~~ **may include**, but is not limited to: a) Identifying **where relevant and based on information reasonably available to the relevant business relationship of the obliged entity** linked, repeated or aggregated behaviour **where such analysis is necessary and proportionate for the identification and assessment of ML/TF risks.** ~~across and within accounts, customers, devices, wallets or other identifiers;~~ b) Analysing risk-relevant behavioural patterns based on an assessment of customer's behaviour, relationships, and transaction patterns over time; c) Recognising network relationships or behavioural patterns that may indicate attempts to conceal ownership, control or the economic purpose of an activity; d) Recognising situations where individual transactions and activities may appear low-risk on their own but form concerning patterns or behaviours over time, including cases where value is accumulated, split, or transferred across multiple transactions and activities.	*Opening paragraph* AFME proposed changes to confirm that the list is non-exhaustive and not mandatory in all circumstances. *Linked, repeated or aggregated behaviour* To clarify that any analysis of linked, repeated or aggregated behaviour should be undertaken on a risk-based and proportionate basis and should not be interpreted as creating a general expectation to perform entity-linkage analysis, potentially across customers or at group level. This may go beyond the AMLR and such an expectation or interpretation could require significant sophisticated operational and technological capabilities, particularly for large cross-border institutions. AFME therefore recommends clarifying that such expectations apply only where relevant, legally permissible , proportionate and supported by reasonably available information to avoid an overly broad interpretation.	AFME proposes replacing '*includes, but is not limited to*' with '*may include, but is not limited to*' to '*linked, repeated or aggregated behaviour'.* AFME also proposes replacing paragraph 44(a) with '*Identifying, where relevant and based on information reasonably available to the relevant business relationship of the obliged entity, linked, repeated, or aggregated behaviour where such analysis is necessary and proportionate for the identification and assessment of ML/TF risks'*
49	Obliged entities should maintain, and where needed, calibrate their monitoring ~~framework~~ **system** to ensure it remains effective ~~and produces valid and meaningful output~~. When designing and adjusting their monitoring ~~framework~~ **system**, obliged entities should consider the potential impact of their choices on both detection capability and the risk of undetected activity. Obliged entities should document, test and record any updates to their detection logic, underlying configuration and, where relevant, models or behavioural baselines, and ensure that these updates are communicated to the relevant staff directly involved in the design, operation or assessment of the monitoring ~~framework~~ **system**.	*Valid and meaningful output* While obliged entities can design, calibrate, test and maintain monitoring frameworks to support effective detection and risk management, they cannot objectively ensure that outputs will possess predefined qualitative characteristics. The Guidelines should instead focus on the effectiveness and appropriate calibration of the monitoring framework and on whether outputs are used to support its ongoing assessment and refinement. AFME also recommends replacing the term *'framework'* with *'system'* throughout paragraph 49. *Framework vs system* The term *'framework'* generally encompasses a broader set of governance arrangements, policies, procedures and controls,	AFME suggests deleting the reference to *'valid and meaningful output'*. AFME propose replacing references to framework with '*system'*.

		whereas the activities described in paragraph 49 relate specifically to the calibration, configuration, testing and maintenance of monitoring systems. Using *'system'* would therefore provide greater precision and consistency with the operational activities addressed in this paragraph.	
51	Obliged entities should ensure that their customer due diligence processes including, sanctions screening processes, and their monitoring framework operate in a~~n integrated and~~ coordinated consistent and risk-based manner and are supported by adequate data and information quality. 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.	Reference to operating in an '*integrated*' manner is proposed for removal as the supervisory objective should be that customer due diligence processes including, sanctions screening processes, and their monitoring framework operate in a coordinated and effective manner and inform one another. The term '*integrated*' may be interpreted as requiring specific technical or organisational integration across systems and controls, which may be disproportionate and unnecessary to achieve the intended risk management outcome.	Deleting the reference to operating in an '*integrated*' manner.
53	Obliged entities should use customer profiles for their monitoring framework and ensure these profiles are based on ~~verified~~ **relevant** customer due diligence information held by them. This should include the customer's purpose and intended nature of the business relationship and, where relevant, the expected transactions and envisaged activities, and the resulting expected behavioural profile of the customer. Where the obliged entity has structurally limited or no access to transaction and activity data, the customer profile should instead draw on other risk-relevant information, such as those arising from the business relationship. 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 time frame** ~~without undue delay.~~	Reference to '*verified*' customer due diligence information may be interpreted as requiring all information used to construct a customer profile to be subject to verification measures, whereas many of the data points referenced in this paragraph, such as the purpose and intended nature of the relationship, expected transactions and other points are not ordinarily part of the customer due diligence requirements subject to verification measures. The focus should be on the use of relevant customer due diligence information available to the obliged entity.	AFME suggests deleting the reference to '*verified*' customer due diligence information AFME propose to replace *'without undue delay'* with '*within a reasonable time frame'*.
56	Obliged entities should have mechanisms in place to ensure that ~~customer or~~ customer-group profiles, including expected transaction and activity profiles and the composition of any reference or peer groups, are kept up to date **on a risk-based and proportionate basis**. ~~This should include reviewing, and where necessary, updating these profiles where monitoring outputs or other information indicate a material change in risk, behaviour or use of the service, regardless of whether a periodic customer review is due.~~	*Customer profiles* The reference to '*customer or.... profiles'* may be interpreted as requiring firms to maintain and update monitoring profiles at individual customer level. Monitoring frameworks are often calibrated using customer segments, risk categories, peer groups or other risk-based groupings. The Guidelines should focus on customer group profiles rather than individual customer-level profiling which is covered under Guidelines 1. *Up-to-date*	*Customer profiles* The reference to '*customer or' deleted'.* *Up-to-date* AFME propose adding ' *on a risk-based and proportionate basis'* following *'kept up to date'.* *Event trigger reviews*

		The guidelines should clarify that monitoring profiles are maintained on a risk-based and proportionate basis. Updates should be required where material changes in ML/TF risks, typologies, customer behaviour or regulatory expectations indicate that calibration or profile adjustments are necessary. AFME propose adding ' *on a risk-based and proportionate basis'* following *'kept up to date'.* *Event trigger reviews* Proposed changes are to avoid conflating monitoring framework maintenance with customer-level event-driven reviews covered under Guidelines 1. The drafting may be interpreted as creating additional event-driven review triggers whenever monitoring identifies changes in risk or behaviour. The focus of this paragraph should remain on maintaining monitoring profiles rather than introducing customer review obligations.	AFME propose removal of *'This should include reviewing, and where necessary, updating these profiles where monitoring outputs or other information indicate a material change in risk, behaviour or use of the service, regardless of whether a periodic customer review is due.'*
57	Where obliged entities identify **material** deviations or inconsistencies, they should reassess the customer's information and risk profile ~~and determine, based on the analysis performed, whether a suspicious activity report should be submitted in accordance with Article 69 AMLR.~~ **Where the assessment gives rise to potential suspicion of money laundering, terrorist financing or related criminal activity, obliged entities should determine whether a suspicious activity report is required in accordance with Article 69 AMLR**	AFME suggests clarifying that not all deviations or inconsistencies identified through monitoring warrant a reassessment of the customer's information and risk profile or a specific assessment of reporting obligations under Article 69 AMLR. The current drafting may be interpreted as creating an automatic link between the identification of any deviation, customer profile reassessment and consideration of SAR reporting. In practice, monitoring frameworks generate a range of outputs, many of which may be explained through routine activity and do not indicate elevated ML/TF risk. Obliged entities should therefore first assess the significance and materiality of any identified deviation or inconsistency and determine the appropriate follow-up action based on the outcome of that assessment. AFME also considers that the current wording risks conflating monitoring outcomes, event-driven customer reviews and SAR assessment processes. While monitoring outputs may, where appropriate, lead to a reassessment of customer information or consideration of reporting obligations, these steps should be driven by the outcome of the analysis performed and the presence of indicators of elevated risk or suspicion, rather than	AFME propose adding '*material'* between '*identify…. deviations'*, replacing '*and determine, based on the analysis performed, whether a suspicious activity report should be submitted in accordance with Article 69 AMLR.*' With '*Where the assessment gives rise to potential suspicion of money laundering, terrorist financing or related criminal activity, obliged entities should determine whether a suspicious activity report is required in accordance with Article 69 AMLR***.'**

		being triggered automatically by any deviation or inconsistency identified through monitoring.	
59	Where continuous monitoring cannot be applied due to the nature of the business model or objective legal or technical constraints beyond the control of the obliged entity, obliged entities may perform monitoring at defined stages in the lifecycle of the business relationship, where ML/TF risks may arise or materially change. In such cases, obliged entities should: a) justify the use of this approach; b) document the limitations and the mitigating measures applied; c) demonstrate that the chosen approach ensures an effective level of risk identification and mitigation, commensurate with the limitations identified.	AFME would welcome clarification regarding the scope of this provision, in particular whether it is intended to apply only to situations where continuous post-transaction monitoring cannot reasonably be performed.	No amendment
60	**N/A – Replacement requested**	AFME notes that the AMLR Article 26 does not establish a general obligation to undertake pre-transaction, pre-activity or real-time monitoring. While such measures may be appropriate in specific circumstances, including where required by competent authorities, FIUs or other legal obligations, obliged entities should retain discretion to determine, based on their business-wide risk assessment, which risks are most effectively identified and mitigated prior to execution and which can be managed through effective post-transaction monitoring. AFME is concerned that paragraphs 60-67 could be interpreted as establishing a general expectation that obliged entities apply pre-transaction, pre-activity or real-time monitoring wherever they have the technical ability to assess or intervene prior to execution. Such an interpretation would move beyond a risk-based approach and could create a de facto expectation that ex-ante monitoring forms part of standard monitoring arrangements across a broad range of products and services. In addition, effective transaction monitoring is frequently based on the identification of patterns, behaviours and relationships that emerge over time across multiple transactions. In many cases, meaningful indicators of suspicious activity cannot be identified from a single transaction in isolation and only become apparent through the analysis of cumulative activity. This	Replacement of 60-67 with '*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 monitoring and pre-activity monitoring to those categories of transactions or activities*'

		reinforces the importance of preserving a risk-based approach that allows obliged entities to determine when post-transaction monitoring is the most effective means of identifying and mitigating ML/TF risks. The current drafting may also create tension with other legal and operational requirements. Certain products and payment services are subject to strict execution timelines and legal obligations that may limit the ability of obliged entities to delay, interrupt or review transactions prior to execution. A general expectation of pre-transaction or real-time monitoring could therefore create uncertainty regarding the interaction between these Guidelines and other applicable legal requirements. AFME propose that paragraphs 60-67 are replaced with the following more consolidated and risk-centric framing '*Based on 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 monitoring and pre-activity monitoring to those categories of transactions or activities.*'	
71	Obliged entities should ensure that appropriate measures are taken **within a reasonable time frame** ~~without undue delay~~, including the identification and escalation of unusual or suspicious transactions and activities, including patterns, linkages or cumulative risk indicators identified through monitoring, for further assessment and, where necessary, escalation.	For paragraph 71, see prior AFME commentary regarding the rationale for replacement of '*undue delay'.*	AFME propose to replace '*without undue delay'* with '*within a reasonable time frame'*.
72	Where, due to the nature of the service or objective technical or legal constraints beyond the control of the obliged entity, relevant transaction data becomes available only after they have been carried out, obliged entities should ensure that appropriate post-transaction monitoring measures are applied **within a reasonable time frame** ~~without undue delay,~~ taking into account the nature, timing and completeness of the information available.	For paragraph 72, see prior AFME commentary regarding the rationale for replacement of '*undue delay'.*	AFME propose to replace '*without undue delay'* with '*within a reasonable time frame'*.

73	Where, due to the nature of the service or objective technical or legal constraints beyond the control of the obliged entity, post-transaction and post-activity monitoring may be limited in scope or duration, obliged entities should ~~ensure that such limitations do not create gaps in their ability to identify, analyse and escalate ML/TF risks~~ **document those limitations, assess the associated ML/TF risks and implement appropriate mitigating measures**. Such limitations should not arise from, or be ~~reinforced~~ **exacerbated** by, ~~the design of products, services or business practices, which should support the effective application of monitoring measures and should not unduly restrict it.~~ **aspects of products, services, or business practices that are within the obliged entity's control**. Legal or technical constraints '**unless external'** should not be used to justify the absence or limitation of post-transaction or post-activity monitoring where the obliged entity is able to identify and analyse transactions and activities after their execution.	AFME supports AMLA's objective of ensuring that limitations affecting post-transaction or post-activity monitoring do not create unmanaged ML/TF risk. However, paragraph 73 would benefit from greater clarity regarding the circumstances in which monitoring limitations may legitimately arise. AFME considers this a more risk-based and operationally realistic approach. Certain monitoring limitations cannot be eliminated, particularly where they arise from external legal, technical or market infrastructure constraints. In such cases, supervisory expectations should focus on identifying, understanding, documenting and mitigating the resulting risks rather than requiring the limitation itself to be removed. This amendment recognises that monitoring constraints may arise from factors beyond the obliged entity's control, including external legal requirements, market infrastructure arrangements and third-party operating models. The current drafting risks implying that any limitation in post-transaction monitoring is a deficiency, despite long-standing supervisory recognition that some business models contain inherent monitoring constraints. AFME further recommends revisiting the final sentence '*Legal or technical constraints should not be used to justify the absence or limitation of….*'. While obliged entities should not rely on internal or self-imposed constraints to justify inadequate monitoring, the drafting does not sufficiently distinguish between internal limitations and externally imposed legal or technical restrictions. In some circumstances, legal constraints may legitimately limit access to information or the operation of monitoring controls. AFME therefore recommends clarifying that the restriction applies only to constraints within the obliged entity's control and that externally imposed limitations may be acceptable where they are understood, documented and mitigated through appropriate alternative controls.	AFME's proposed amendments replace the requirement that obliged entities '*ensure that such limitations do not create gaps in their ability to identify, analyse and escalate ML/TF risk'* with a requirement to '*document those limitations, assess the associated ML/TF risks and implement appropriate mitigating measures.'* AFME also proposes replacing the statement that '*Such limitations should not arise from, or be reinforced or exacerbated by, the design of products, services or business practices, which should support the effective application of monitoring measures and should not unduly restrict it'* with '*aspects of products, services, or business practices that are within the obliged entity's control'.* Following '*Legal or technical constraints'* add '*unless external'.*
75	Obliged entities should ensure that monitoring outputs, whether generated through automated systems or arising from manual processes within the monitoring framework, are assessed ~~without undue delay~~ **within a reasonable timeframe**, prioritised based on risk, and escalated, where further analysis is required, to staff with appropriate	For paragraph 75, see prior AFME commentary regarding the rationale for replacement of '*undue delay'.*	AFME propose to replace '*without undue delay'* with '*within a reasonable time frame'*.

	knowledge of the customer and expertise. Obliged entities should be able to explain, on request, how monitoring outputs were assessed, escalated and acted upon, including the documented rationale for decisions taken.		
76	Obliged entities should define and maintain appropriate internal arrangements to ensure that monitoring outputs are assessed and resolved **within a reasonable time frame** ~~without undue delay~~, including mechanisms to identify, monitor and address any accumulation of pending monitoring outputs that may affect the effectiveness of the monitoring framework.	For paragraph 76, see prior AFME commentary regarding the rationale for replacement of '*without undue delay'.*	AFME propose to replace *'without undue delay'* with '*within a reasonable time frame'*.
83	83. Obliged entities should define the outcomes of their monitoring framework and periodically reassess whether those outcomes remain appropriate in light of their business-wide risk assessment ~~and, where relevant, publicly available national or Unionlevel priorities~~.	AFME considers that references to '*define the outcomes'* may create ambiguity regarding the extent of an obliged entity's responsibilities. While obliged entities should ensure that their monitoring frameworks, controls and processes are appropriately designed, implemented and operating effectively, they cannot guarantee particular outcomes, as these may depend on factors outside their control, including customer behaviour and the nature of the activity being monitored. AFME recommends using terminology that is consistent with the remainder of the Guidelines and focusing supervisory expectations on the effectiveness of monitoring frameworks and controls rather than on the achievement of specific outcomes. This would provide greater legal certainty regarding the obligations placed on obliged entities and better reflect the risk-based nature of AML/CFT controls. AFME members are not clear what '*union level priorities'* refers to and, given the ambiguity of the term, recommend its removal.	Removal of '*and, where relevant, publicly available national or Union level priorities*'. '
86	Obliged entities should ensure that the responsibility for overseeing the effectiveness of the monitoring framework is clearly assigned and that identified deficiencies are addressed **in a reasonable timeframe** ~~without undue delay.~~ Governance arrangements, including policies and procedures, should enable relevant staff to effectively understand and challenge monitoring tools and their outputs.	For paragraph 86, see prior AFME commentary regarding the phrase '*undue delay*'.	AFME propose to replace *'without undue delay'* with '*within a reasonable time frame'*.
87	Obliged entities **may consider** ~~should assess~~ whether the use of automated or advanced analytical tools, including algorithms, machine learning, artificial intelligence and other	*Undue delay*	*Undue delay*

	innovative technologies, would enhance the effective identification and escalation of ML/TF risks within their monitoring framework. This assessment should take into account whether manual processes are sufficient to achieve effective monitoring ~~outcomes~~, having regard to the obliged entity's risk exposure, complexity, size and operational scale, including the volume and speed of activity. The deployment of such tools should not, in itself, be considered an indicator of effectiveness. Effectiveness should instead be assessed by reference to whether the tools enable the obliged entity to detect and escalate relevant ML/TF risks **within a reasonable time frame**. ~~without undue delay.~~	See prior AFME commentary regarding the phrase '*undue delay*'. AFME propose removal of '*outcomes*' as per paragraph 83 commentary. *May consider the use of automated or advanced analytical tools* 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. *Outcomes* See prior commentary regarding the term outcomes.	AFME propose to replace '*without undue delay*' with '*within a reasonable time frame*'. *May consider the use of automated or advanced analytical tools* The addition of '*may consider*' in place of '*should assess*'.

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

(i)specify the paragraph concerned;	**AFME amendments to AMLA paragraphs**	**(ii)explain your rationale; and**	**iii)consider submitting an amendment proposal**
78	Obliged entities that use automated **or semi-automated** mechanisms to **support the investigation, assessment or closure of monitoring outputs** ~~close monitoring outputs~~ should ensure ~~that these mechanisms are only applied to cases which, following automated analysis, do not indicate suspicious or unusual transactions and activities or other material ML/TF risk indicators.~~ should ensure that **such mechanisms are underpinned by a documented and explainable decision logic, proportionate safeguards, and effective human oversight, calibrated to the case's specific level of risk.** ~~Such mechanisms should not be applied where there are indicators of heightened risk., including in relation to higher-risk customers or situations requiring enhanced scrutiny.~~ **The use of automated or semi-**	AFME supports AMLA's objective of ensuring that the use of automated or semi-automated mechanisms within monitoring frameworks is appropriately governed and subject to effective safeguards. However, we consider the current drafting to be unnecessarily restrictive and not fully reflective of the increasingly important role that automation plays in effective and risk-based monitoring frameworks. This amendment recognises that automation can assist at multiple stages of the monitoring process and should not be viewed solely as a tool for alert closure. AFME considers that the appropriateness of automation should be determined by the design, governance and controls surrounding the process rather than by a prescriptive exclusion of particular	AFME proposes replacing the references to mechanisms that '*close monitoring outputs*' with mechanisms that '*support the investigation, assessment or closure of monitoring outputs'.* AFME also proposes removing the restriction that such mechanisms should only be applied where outputs '*do not indicate suspicious or unusual transactions and activities or other material ML/TF risk indicators'* and replacing it with the requirement 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.*'

	automated mechanisms for such purposes should not, in itself, be restricted 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.	categories of alerts. Risk-sensitive deployment of automation can enhance the consistency, effectiveness and scalability of monitoring processes while allowing human expertise to be focused on higher-risk matters. AFME believes that customer risk classification alone should not automatically preclude the use of automation and note this is not required under the AMLR. The determining factor should instead be whether the automated process is appropriately calibrated, explainable, subject to effective oversight and supported by safeguards commensurate with the risk. This approach is more consistent with a risk-based framework and will allow firms to leverage technological solutions where appropriate while maintaining effective management of ML/TF risk.	AFME also proposes deleting '*Such mechanisms should not be applied where there are indicators of heightened risk, including in relation to higher-risk customers or situations requiring enhanced scrutiny*' and replacing it with '*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.*'
87	Obliged entities should assess whether the use of automated or advanced analytical tools, including algorithms, machine learning, artificial intelligence and other innovative technologies, would enhance the effective identification and escalation of ML/TF risks within their monitoring framework. This assessment should take into account whether manual processes are sufficient to achieve effective monitoring ~~outcomes~~, having regard to the obliged entity's risk exposure, complexity, size and operational scale, including the volume and speed of activity. The deployment of such tools should not, in itself, be considered an indicator of effectiveness. Effectiveness should instead be assessed by reference to whether the tools enable the obliged entity to detect and escalate relevant ML/TF risks **within a reasonable time frame**. ~~without undue delay.~~	On paragraph 87, AFME recommends that the Guidelines explicitly recognise the interaction between AML/CFT requirements under the AMLR framework and applicable EU data protection requirements, particularly where obliged entities deploy advanced analytical tools, machine learning or artificial intelligence solutions. The design, deployment and governance of such technologies require compliance with both AML/CFT and data protection obligations.	AFME propose to replace '*without undue delay*' with '*within a reasonable time frame*'.

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?

- Increase of compliance costs and operational processes **50-75%**
- Reduction of compliance costs and operational processes
- No effect

Methodology
This assessment is based on feedback from AFME member firms regarding the operational, technological and compliance implications of implementing the requirements in Guideline 2, drawing on firms' experience of transaction monitoring programmes, large-scale AML/CFT transformation projects, and the use of third-party monitoring and compliance service providers.
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;					X
implications for staff;				X	
other (please specify) – **Client impact, TM systems**				X	

AFME Response
AFME expects the requirements set out in Guideline 2 to result in a significant increase in compliance costs and operational processes (estimated at 50-75%). This assessment is primarily driven by the introduction of real-time, pre-transaction, and pre-activities monitoring requirements, which represent a substantial departure from the transaction monitoring frameworks currently operated by many firms.

As drafted, the requirement to conduct monitoring and assessment activities prior to transaction execution raises significant operational, technological and practical challenges. Existing AML/CFT transaction monitoring frameworks are generally designed to identify unusual or suspicious activity through risk-based analysis of completed transactions over time. In practice, transaction monitoring systems typically assess transaction patterns, behaviours and risk indicators across customer activity over time and therefore operate differently from pre-transaction controls applied to individual transactions. While firms already operate certain pre-transaction controls, such as sanctions screening, transaction filtering, fraud prevention measures and certain trade finance controls, these controls serve different purposes and operate independently from AML/CFT transaction monitoring systems. The implementation effort associated with the draft Guidelines therefore arises primarily from the potential need to redesign existing transaction monitoring frameworks to operate prior to transaction execution, rather than from enhancements to existing pre-transaction control processes.

Even if firms were able to adapt existing transaction monitoring frameworks to operate prior to transaction execution, the implementation effort would be considerable. Firms would need to make extensive changes to transaction monitoring systems, customer lifecycle management platforms, payment infrastructure and associated controls. The proposed requirements would also necessitate significant involvement from technology, change management, operations, compliance and business teams.

In addition, many firms rely on third-party vendors and outsourced service providers for aspects of their transaction monitoring and customer due diligence frameworks. These providers would also need to adapt their systems and services to support the proposed requirements. Given the scale of the expected changes and compressed implementation timelines, firms anticipate a material increase in vendor costs, implementation expenditure and ongoing operational expenses.

AFME is also concerned about the potential impact on customers. Real-time pre-transaction assessments may introduce transaction delays, increased requests for information and a higher volume of customer interventions, particularly where alerts require manual review before transactions can proceed. This could negatively affect customer experience and create friction in legitimate business activity.

For these reasons, AFME has assessed the impact on processes and controls as very negative, reflecting the extensive redesign of existing monitoring frameworks required. The impact on staff is assessed as negative due to the additional compliance, operational and investigative resources likely to be needed to manage increased alert volumes and intervention requirements. The impact on client experience and transaction monitoring systems is also assessed as negative, reflecting both the significant technology changes required and the potential disruption to customer journeys.

While AFME supports the objective of strengthening financial crime controls, we encourage AMLA to further consider the operational feasibility, proportionality and implementation implications of introducing real-time pre-transaction monitoring requirements, particularly given the extensive systems changes, resource commitments and customer impacts that would result from the current drafting.

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.

Dormant or restricted
The guidance and examples provided appear to focus primarily on standard customer offboarding scenarios and do not address situations where an obliged entity is unable both to complete CDD remediation and to terminate the business relationship.

In practice, obliged entities may be subject to long-term contractual arrangements, such as committed credit facilities or other irrevocable obligations, where a customer is unwilling to cooperate with a periodic review but the institution has no contractual right to terminate the relationship. In such cases, immediate offboarding may expose the institution to legal and litigation risk, while opportunities to obtain updated information may be limited.

The guidance should reference circumstances where a relationship is effectively dormant or restricted, with no normal business activity taking place but residual contractual obligations remaining. As a concrete drafting proposal AFME requests explicit confirmation that obliged entities may apply a risk-based approach in such scenarios.

AFME contacts

Louise Rodger, Managing Director, Compliance, Control and Accounting
Louise.rodger@afme.eu

Stefano Mazzocchi, Managing Director and Deputy Head Advocacy
Stefano.mazzocchi@afme.eu

Hanna Sowemimo, Associate Director, Compliance, Control and Accounting
Hanna.sowemimo@afme.eu

Ria Mehta, Associate, Compliance, Control and Accounting
Ria.mehta@afme.eu