EDPIA
The European Digital Payments Industry Alliance

EDPIA's answer to AMLA Consultation Paper - Draft Regulatory Technical Standards under Article 28(1) of Regulation (EU) 2024/1624

May 2026

Section 2 - Substantive comments on the draft Regulatory Technical Standards

1. Do you agree that the proposals set out in these draft RTS can be applied across the range of products and services provided by your obliged entity?

The European Digital Payments Industry Alliance (EDPIA) welcomes the recognition of eIDAS-based identification solutions as a modality for remote customer onboarding, while noting that the framework should allow for the use of multiple secure solutions and that one overarching solution is not sufficient and raises multiple challenges.

EDPIA believes that preserving technological neutrality for customer onboarding processes is essential and can likewise contribute to a risk-based approach to client risk management. We therefore remain cautious with the draft Regulatory Technical Standards, more precisely Article 7, which uses mandatory language ("shall") to impose eIDAS-based solutions as the primary identification method, with Article 7(2) permitting alternatives only where eIDAS "is not available or cannot reasonably be expected to be provided", and Article 7(4) further requiring per-customer justification of why each customer could not be verified through eIDAS. The combined effect treats eIDAS as the mandatory default and relegates other compliant - and often more risk-relevant - solutions to a fallback of last resort. Such an approach raises serious questions from both an operational and legal perspective, in turn hindering the ability of payment service providers to onboard customers in an efficient manner, especially in cross-border contexts where the relevant competent authority for that per-customer justification is itself unresolved.

To recall, these solutions are not universally available and interoperable at present and will still need time to reach their intended uptake. The European Digital Identity framework only entered into force in May 2024, with Member States required to make at least one EU Digital Identity Wallet available by end of 2026 -just months before the AMLR applies on 10 July 2027. Broad acceptance, cross-border interoperability, and operational stability of eIDAS solutions cannot reasonably be expected by the time this RTS enters into force, and a binding Level 2 instrument should not be set in stone around assumptions that do not yet hold.

In order to ensure that the measures can be properly implemented and do not pose a disproportionate burden or dual-stack problem, EDPIA proposes the following amendments to Article 7, treating eIDAS-based solutions as a recognised high-assurance option rather than a primary legal obligation.

Suggested wording of Article 7 (1, 2 and 4):
(1) Obliged entities may [not "shall"] use electronic identification means meeting the requirements of Regulation (EU) No 910/2014 with regard to the assurance levels "substantial" or "high", or relevant qualified trust services as set out in that Regulation.
(2) In addition, especially where the solution under paragraph 1 is not available or cannot reasonably be expected to be provided, obliged entities shall obtain the natural person's identity document, passport or equivalent using remote solutions that meet the conditions set out in paragraphs 3 and 4.
…
(4) Obliged entities using remote solutions shall be able to demonstrate to their competent authority that the remote verification solutions used comply with this Article. The per-customer justification under Article 22(6) of Regulation (EU) 2024/1624 should be deleted.
New final article -Review clause:
By [date], AMLA shall, in cooperation with the Commission, review the application of Article 7 in light of the maturity and pan-European interoperability of electronic identification means under Regulation (EU) No 910/2014, and submit a report accompanied, where appropriate, by proposals to amend this Regulation.
This proposal builds on a proven approach. The EBA Guidelines on remote customer onboarding (EBA/GL/2022/15) have demonstrated since 2022 that an outcome-based, technology-neutral framework delivers high assurance to remote identification across the Union. The framework is also future-proof: it does not lock in any technology and adapts as new technologies but also threats (e.g. AI-generated synthetic identities) evolve.

2. Do you agree that the proposals set out in these draft RTS allow for the effective application of a risk-based approach towards compliance with AML/CFT requirements?
EDPIA answer:

In line with our answer to Question 1, EDPIA believes that the provisions mandating the use of eIDAS-based solutions undermine the essence of a risk-based approach: by imposing eIDAS through mandatory language and relegating other compliant solutions to a fallback requiring per-customer justification, the draft treats identification as a binary hierarchy rather than a risk-sensitive determination. Robust remote onboarding solutions -including AI/ML-based identity verification meeting or exceeding eIDAS assurance levels, as well as widely used national solutions (such as Denmark's BankID and Belgium's "itsme") -are presumptively non-compliant unless eIDAS is unavailable, regardless of risk. Article 7 as drafted constrains -and arguably contradicts -Article 22(6) AMLR, which recognises both document-based and electronic identification as valid modalities. A Level 2 measure should not narrow options recognised at Level 1.

A further point: eIDAS is an identification instrument, not a ML/TF risk detection tool. It confirms identity at onboarding but does not address whether the customer is a victim of identity theft, a money mule, under coercion, or whether the identity is a synthetic one generated through AI. Current verification solutions -liveness and deepfake detection, document authenticity checks, behavioural biometrics, real-time anomaly detection -are designed precisely to address those risks. Mandating eIDAS as primary and relegating these capabilities to a justified fallback reduces, rather than enhances, risk-relevant information at onboarding. Locking Level 2 around eIDAS therefore embeds a technological bias into the AML/CFT regime, foreclosing the very tools best equipped to address evolving threats -technological neutrality is essential precisely because financial crime evolves faster than any single technology can address.
EDPIA accordingly proposes the drafting amendments to Article 7 set out under Question 1, together with the review clause. These measures align Level 2 with Article 22(6) AMLR, preserve technological neutrality, the risk-based approach, and European competitiveness in payments innovation as already operationalised under EBA/GL/2022/15.

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

EDPIA has identified two main instances where the information required by the draft RTS may not be routinely available and the proposals do not offer alternatives:

(1) Annex I attributes are not consistently available through identity documents and electronic identification means in use across the EU. The list of minimum attributes corresponding to Article 22(1) AMLR -including all names and surnames, place of birth, all nationalities, national ID number, residential address, and tax identification number -does not match the data routinely surfaced by widely used identification means or recorded on physical identity documents accepted across the EU. A review of the Council's PRADO database confirms that not all attributes appear on every document, Member State, or customer category, and those that do appear are not standardised in scope or structure. A further concern is the relationship between Annex I and Article 22(1) AMLR itself: where the AMLR uses qualifiers such as "where available" and "where applicable", Level 2 should reflect that flexibility rather than narrow it. EDPIA proposes recalibrating the Annex I data set so that attributes not consistently available through accepted identification means and of limited AML/CFT value in low-risk scenarios are collected only where the risk profile so requires, not uniformly.

(2) eIDAS-based identification means for cross-border remote onboarding. A substantial share of customers will not have a usable eIDAS at onboarding -particularly from Member States with delayed wallet rollout or low qualified trust service uptake, and from underserved groups (mobile workers and migrants resident outside the Member State issuing their eID; third-country nationals lawfully resident in the EU; older customers; younger customers without an eID). An eIDAS-only default sits uneasily with the EU objectives of financial inclusion. A further consequence is a dual-stack burden: a separate compliant onboarding solution will be required for every customer without a usable eIDAS means, and even where the customer has eIDAS, if it does not surface all Annex I attributes a fallback mechanism will still be required to complete the data set. Our proposed way forward is outlined in our previous answers to Questions 1 and 2.

4. Considering AMLA's legal mandate in Article 28(1) of Regulation (EU) 2024/1624, and taking into account your obliged entities' products offered and service provided, what other simplified due diligence measures should be included in the draft RTS, for example because of the associated lower ML/TF risks of these products and services? Please provide concrete drafting proposals and rationale for the specific measures you would propose.
EDPIA answer:

Concerning the exemption under Article 19(7) Regulation (EU) 2024/1624, and Article 31 of the draft RTS outlining the risk factors to be detailed, EDPIA has identified four areas where targeted amendments would foster a genuine and workable risk-based approach:

(1) **Risk factors must not be cumulative.** The relevant risk factors should be understood as a non-exhaustive list, with supervisors able to consider one or more such factors to determine the extent of the exemption -rather than applying a binary catalogue where each factor must be fulfilled in its entirety. This is essential to allow national competent authorities to apply a genuine risk-based approach and accommodate the diverse business models of e-money issuers.

(2) **Distribution-side and issuer-side risk factors are missing.** Several of the most effective risk-mitigating measures available to e-money issuers focus on the distribution and use of the instrument over its lifecycle, not on the moment of issuance. We propose adding distribution monitoring, merchant monitoring, suspicious-pattern detection with automatic deactivation, and adequate technological safeguards as recognised risk factors. These measures materially mitigate ML/TF risk associated with the distribution and use of e-money products and are demonstrably more risk-relevant than some of the criteria currently envisaged.

(3) **Certain proposed criteria should be reconsidered.** Criteria that effectively replicate elements of the Limited Network/Range exclusion under Article 3(k) of Directive (EU) 2015/2366 risk conditioning the e-money exemption on the product not being e-money at all, which would run counter to the legislative intent of Article 19(7) AMLR. Similarly, criteria focused on the issuer or its distribution infrastructure (rather than on the e-money instrument itself) sit uneasily with AMLA's mandate, which is directed at the instrument.

(4) **Account-based funding should not be a precondition.** Linking the e-money exemption to funds originating from a regulated EEA account would contradict the spirit of the Level 1 text, which is intended to cover current e-money products that are acquired in exchange for coins and banknotes (Recital 13 of Directive 2009/110/EC).

Suggested wording of Article 31:

Where supervisors decide to allow for an exemption under Article 19(7) Regulation (EU) 2024/1624, based on the conditions listed in Article 19(7), points (a) to (d), of Regulation (EU) 2024/1624, supervisors shall consider one or more of the following risk factors to determine the extent of that exemption:
(a) the extent to which the payment instrument has low transaction limits or thresholds to limit transaction values;
(b) the nature of the goods or services that can be acquired, including the level of risks associated with these goods and services;
(c) the extent to which the transactions through the electronic money instrument are executed by an obliged entity that applies customer due diligence measures and record-keeping requirements laid down in Regulation (EU) 2024/1624;
(d) the extent to which the payment instrument is available through direct channels which may include the issuer or a network of service providers which have appropriate safeguards and fraud measures in place;
(e) the extent to which the payment instrument has a limited geographical distribution;
(f) the extent to which the issuer applies adequate technological tools, such as geo-fencing and IP tracking, to monitor access to the payment instrument from, transfers to or receiving funds from countries that are not EU Member States nor EEA countries, in accordance with the applicable laws.
(g) The extent to which the issuer has measures in place that allow for an effective monitoring of the distribution channels of the e-money product in order to detect and prevent suspicious activities.
(h) The extent to which the issuer has measures in place that allow for an effective monitoring of the merchants that accept payments via the e-money product in order to detect and prevent suspicious activities.
(i) The extent to which the issuer has measures in place that allow for the identification of suspicious transaction patterns and behavioral profiling and allows for disabling the payment instrument in case a suspicious activity pattern is detected. Re-activation of the product can only be done by the issuer.
(j) The extent to which the issuer has adequate technological safeguards in place. Such measures could include device fingerprinting and IP address tracking to detect suspicious activity or the use of velocity checks (e.g. number of transactions in a short period).

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

EDPIA wishes to flag a cross-cutting observation relevant to the draft RTS as a whole. The article-specific concerns raised under Questions 1–4 share a common thread: ensuring that the implementing standards reflect the flexibility expressly recognised at Level 1 -including the document-based and electronic identification modalities under Article 22(6) AMLR, the "where available" and "where applicable" qualifiers in Article 22(1) AMLR, and the genuinely risk-based logic of Article 19(7) AMLR. EDPIA would welcome a recital in the RTS reaffirming that obliged entities and competent authorities are to apply these standards consistently with the risk-based and technology-neutral approach the AML Regulation operationalises, providing a stable interpretative anchor over the lifetime of the RTS and helping to avoid divergent national interpretations. In line with this, recognising the existing outcome-based, technology-neutral framework that has been in operation across the financial sector since 2022 alongside Article 7 -rather than displacing it - would preserve technological neutrality, support European competitiveness in payments innovation, and ensure that the measure is no more restrictive than necessary to achieve the AML/CFT objective.

Section 4 - Overall assessment

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

(x) Somewhat inadequate

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

One-off implementation costs - *(x) Managable impact*
Recurrent costs - *(x) Managable impact*

Please justify your answer to the previous question and provide evidence where possible:

As long as eIDAS solutions are not universally available and interoperable, obliged entities will be compelled to maintain parallel onboarding infrastructures that present material costs disproportionate to any potential risk reduction achieved. To illustrate the order of magnitude: in the remote retail onboarding segment, a per-customer cost increase of even a few euros translates into millions of euros at the scale of a typical user base, and the binding default under Article 7 would add to -not replace - existing onboarding costs that obliged entities have already invested in compliant solutions. Even when pan-European interoperability eventually matures, truly integrated cross-Member-State solutions will realistically be within reach of only a small number of large-scale operators, raising legitimate concentration concerns. Moreover, even assuming full interoperability of eIDAS solutions and the emergence of intermediary service providers capable of facilitating pan-European integration, the expectation that the entirety of the obliged entity population -significantly expanded under the AML Regulation - could realistically complete such integrations within the applicable transitional timeframes appears difficult to substantiate, particularly with respect to smaller and newly in-scope entities operating with inherently limited technical and compliance resources.