Electronic Money Association
67 Square Marie-Louise
Brussels 1000
Belgium
www.e-ma.org

AMLA
(response submitted online)

3 September 2026

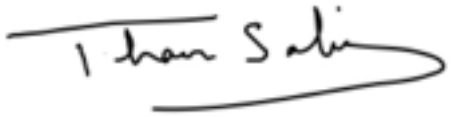
Dear Madam/Sir,

Re: EMA response to Consultation Paper on the Draft Guidelines on ongoing monitoring of a business relationship under Article 26(5) of Regulation (EU) 2024/1624

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide, providing online payments, card-based products, electronic vouchers, cryptoasset services and mobile payment instruments. Most members operate across the EU, most frequently on a cross-border basis. A list of current EMA members can be accessed here.

I would be grateful for your consideration of our comments and proposals.

Yours sincerely,



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

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?

EMA comments:

We welcome the risk-based approach to updating customer due diligence measures, including the confirmation that expired identity documents need not be re-collected as a matter of course, but only where this is warranted by an appropriate risk assessment. We also support the principle set out in paragraph 2 that an early review- whether event-driven or conducted proactively - may reset the timetable for the next periodic update. This is an important foundation for entities that rely on continuous monitoring frameworks.

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?

EMA comments:

Paragraphs 30 onwards refer to the "temporary" suspension of transactions where requested documents or information have not been received, but the permitted duration of such a suspension is not defined. This may result in inconsistent approaches and potentially prolonged restrictions on customers. Timeframes should allow for a risk-based approach, taking into account the nature of the missing information, the level of ML/TF risk and any applicable legal or operational constraints.

Question 3: 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? Specifically, please provide an estimate of: a) the one-off and ongoing costs; b) the impact on IT systems and other internal processes; c) any other impact you might identify.

EMA comments: No comment.

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

EMA comments:

Paragraph 34(e) states that the monitoring framework must be 'capable of identifying patterns, behaviours or linkages that may indicate risks related to *the non-implementation or evasion of targeted financial sanctions*.' This requirement exceeds the obligations in Level 1 text, as neither the AMLR nor sanctions legislation require the use of the ongoing monitoring framework (vs. business-wide risk assessment and management processes) for sanctions evasion risk. We therefore recommend deleting this statement. While we fully support mitigating sanctions evasion and leveraging transaction-monitoring systems where appropriate, mandating the ongoing monitoring framework as the core mechanism is overly prescriptive. In practice, the primary mitigating measure remains robust name screening, extended to intermediate shareholders pursuant to Article 20(1)(d) AMLR. Indicators of sanctions evasion may also be detected when reviewing transactions triggered by risk-based monitoring rules, for example, transfers involving high-risk jurisdictions associated with sanctions evasion. Effective detection in such cases may depend significantly on targeted staff training rather than automated identification of patterns or linkages. Obliged entities should therefore retain flexibility to address sanctions-evasion risks through their broader risk-management processes.

It is unclear in what situation an obliged entity may use post-transaction monitoring rather than pre-transaction or real-time monitoring. In paragraph 61, the reference to an obliged entity's "ability to assess or intervene" is broad and could imply that any technical capacity to stop a transaction creates an expectation to monitor it before execution.

Most PSPs conduct transaction monitoring primarily on a post-transaction basis to avoid unduly delaying legitimate payments while alerts are investigated. This is particularly relevant for high-volume or instant payments, where pre-transaction monitoring could generate delays and customer detriment. Certain risks may also only become apparent through transaction patterns or information available after execution.

The Guidelines should therefore clarify that PSPs may use post-transaction monitoring where justified by factors such as payment execution timeframes, transaction speed and volume, system architecture, the PSP's role and access to information, and the likely impact of false positives. They should also confirm that the mere technical ability to stop a transaction does not automatically make pre-transaction monitoring mandatory, and that obliged entities may apply an appropriate risk-based combination of pre- and post-transaction controls.

Paragraph 66 should be revised to recognise that the appropriateness of pre-transaction, pre activity or real-time monitoring depends on the obliged entity's business model and other relevant factors, including proportionality, operational feasibility and potential customer detriment. While we acknowledge that limitations should not create coverage gaps or stem from poor product design (as symmetrically reflected for post-transaction monitoring in Para 73), the text should avoid suggesting that legitimate products or business models must be redesigned solely to accommodate pre-transaction monitoring where effective alternative post-transaction controls are available. The wording regarding "objective legal or technical constraints beyond the obliged entity's control" should be clarified to ensure obliged entities retain the flexibility to implement balanced ex-ante and ex-post controls based on their actual capacity to act.

We would welcome confirmation that, where an obliged entity facilitates or initiates a transaction or activity but does not directly execute or control the final transfer due to the use of smart-contract intermediated settlement, paragraphs 64-66 permit the obliged entity to adopt an alternative monitoring approach. This may include post-transaction and event-driven monitoring, supported by on-chain analytics, as the primary monitoring control, where the obliged entity is not able, within its role, business model and access to relevant information, to assess or intervene prior to the transaction being carried out or completed.

This should be subject to the obliged entity documenting the relevant legal or technical constraints, applying pre-service or pre-activity controls where feasible, including CDD, wallet/address screening, review of instructions and assets involved, and demonstrating that the overall framework remains effective in identifying, assessing and escalating ML/TF risks.

It would be helpful for AMLA to elaborate further on its expectations for data testing. The draft text of paragraph 82 currently remains high-level, and additional guidance specifying minimum outcomes as to what is expected when conducting data tests would be very welcome. In particular, AMLA should clarify the expected scope, methodology, frequency, data-quality criteria, documentation and remediation of identified deficiencies, as well as how these requirements should be applied proportionately to obliged entities of different sizes, risk profiles and levels of complexity.

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?

EMA comments:

EMA supports the use of automated and advanced analytical tools, including AI, where they demonstrably improve ongoing monitoring. However, it should be clarified to what extent is using such tools becoming mandatory.

The Guidelines should distinguish between an obligation to assess the suitability of these tools and an obligation to implement them. An obliged entity should be able to conclude, on a risk based basis, that advanced automation or AI is not proportionate to its size, business model, transaction volumes, complexity or ML/TF/PF risk exposure.

This is particularly important for smaller or less complex firms, for which rules-based systems or manual controls may remain effective. Advanced tools may also introduce costs and risks relating to data quality, explainability, information security, third-party dependency and human oversight.

The guidelines, therefore, should not impose a standalone requirement to use AI or advanced analytical tools. They should also clarify that supervisors should assess the effectiveness of monitoring arrangements and not the use of any particular technology.

Paragraph 91 requires obliged entities relying on third-party providers to ensure that sufficient information is available to meet the requirements concerning oversight, challenge and explainability. However, it is unclear what constitutes "sufficient information" where commercially available tools, including blockchain analytics platforms, incorporate proprietary algorithms or machine-learning models.

While paragraph 90 confirms that full technical interpretability of the underlying model is not required, it should clarify that an obliged entity may satisfy this requirement where it can understand, document, explain and appropriately challenge the tool's role, functioning, outputs, material assumptions and limitations; assess its suitability and performance; and maintain effective governance and human oversight. This should not require access to source code, model parameters, training data or other proprietary intellectual property.

Question 6: What impact would the design and implementation of the transaction and activity monitoring framework described in Guideline 2 have on your compliance costs? Specifically, please provide an estimate of: a) the one-off and ongoing costs; b) the impact on IT systems and other internal processes; c) any other impact you might identify.

EMA comments: No comment.

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

EMA comments:

The use of the term "materially" without further elaboration or definition could give rise to a wide variety in national interpretation. For instance, it is currently unclear when deficiencies in data quality, accuracy, attribution or completeness should be taken to "*materially* affect monitoring outcomes" and therefore should be documented and mitigated (para. 93). Or when a monitoring framework can be taken as being capable of identifying transactions and activities "that *materially* deviate from expected behaviour" (para. 34(d)). Or when risk "*materially* changes," requiring monitoring (para. 59). We recommend that rather than using the term "materially" AMLA describe the precise outcome that is to be achieved or avoided.

Members of the EMA as of September 2026

Airbnb Inc
Aircash
Airwallex (UK) Limited
Amazon
American Express
Banked
BCB Digital Ltd
Bitstamp
Blackhawk Network EMEA Limited
Boku Inc
Booking Holdings Financial Services International Limited
BVNK
Bytedance Payments
Cardaq Ltd
CashFlows
Circle
Coinbase
Crypto.com
Currenxie Technologies Limited
Decta Limited
Deel
eBay Sarl
ECOMMPAY Limited
emerchantpay Group Ltd
EML Payments
EPG Financial Services Limited
eToro Money
Etsy Ireland UC
Euronet Worldwide Inc
Finance Incorporated Limited
Financial House Limited
FinXP
First Rate Exchange Services
MuchBetter
myPOS Payments Ltd
Navro Group Limited
Newrails, UAB
Nium Solutions Limited
Nuvei Financial Services Ltd
OFX
OKX
OpenPayd
Owl Payments Europe Limited
Own.Solutions
Papaya Global / Azimo
Park Card Services Limited
pay.cetera B.V.
Payhawk Financial Services Limited
Paymentsense Limited
Payoneer Europe Limited
PayPal
Paysafe Group
Paysend EU DAC
Peratera UK Ltd
Plaid B.V.
Pleo Financial Services A/S
PPS
Push Labs Limited
Remitly
Revolut
Ripple
Satispay Europe S.A.
Securiclick Limited
Segpay
Soldo Financial Services Ireland DAC
Square

Fiserv
Flywire
Globepay Limited
GoCardless Ltd
Google Payment Ltd
IDT Financial Services Limited
iFAST Global Bank Limited
Imagor SA
Kraken
Loodapay LU S.A.
Modulr Finance B.V.
MONAVATE
MONETLEY LTD
Moneyhub Financial Technology Ltd
Moorwand Ltd
Stripe
SumUp Limited
Syspay Ltd
TransactPay
TransferGo Ltd
TransferMate Global Payments
TrueLayer Limited
Uber BV
Unzer Luxembourg SA
Vitesse PSP Ltd
VIVA WALLET.COM LTD
Weavr Limited
WEX Europe UK Limited
Wise
WorldFirst