

Comments reflected in electronic submission at eba.europa.eu

June 6, 2025

European Banking Authority
Tour Europlaza
20 avenue André Prothin
CS 30154
92927 Paris La Défense CEDEX
France

RE: Crypto Council for Innovation Response to Consultation on Proposed RTS in the context of the EBA's Response to the European Commission's Call for Advice on New AMLA Mandates

The [Crypto Council for Innovation](#) (CCI) appreciates the opportunity to provide comments on the [four draft Regulatory Technical Standards](#) (RTSs) proposed as part of the European Banking Authority's (EBA) response to the European Commission's Call for Advice regarding mandates for the newly established Anti-money Laundering Authority (AMLA).

CCI is a global alliance of industry leaders within the digital assets industry and is committed to promoting the advantages of digital assets while showcasing their potential for transformation. [CCI's members](#) represent various sectors within the digital asset ecosystem and share a common objective: advocating for responsible global regulation of digital assets to unlock economic opportunities, enhancing quality of life, promoting financial inclusivity, safeguarding national security, and countering illicit activities. CCI firmly believes that achieving these objectives necessitates well-informed, evidence-driven policy choices achieved through collaborative participation. We are committed to supporting the EU's objectives of financial integrity and the prevention of money laundering and terrorist financing.

CCI commends the EBA's efforts to establish technical standards for a consistent AML supervisory framework. We generally welcome the shift toward a harmonized regulatory architecture at EU level (as opposed to diverging national standards) through the AML legislative package. Harmonized provisions, however, need to be consistently applied in a risk-based manner, whilst respecting the principle of proportionality. As such, AMLA's work can promote the purported political objective of streamlining - and thus lightening - the administrative burden for crypto-asset service providers (CASP) in the EU.

This consultation is a critical opportunity to shape how AMLA, as a newly founded authority, and national competent authorities (NCAs) supervise and assess CASPs. While we strongly support consistent, proportionate, and technology-neutral AML/CFT standards, we believe that

key clarifications and adjustments are needed to ensure the RTSs are workable in practice and aligned with the risk-based approach that underpins EU AML policy.

Against this backdrop, CCI urges the EBA to reconsider various factors and thresholds included in the draft RTSs. In addition to general concerns regarding Customer Due Diligence (CDD) and remote onboarding provisions, without further calibration, the draft RTSs risk disproportionately affecting CASPs due to:

- Over-generalized risk classification approaches;
- Inappropriate assumptions based on traditional finance models;
- A lack of recognition for crypto-native compliance tools and risk mitigants.

We are particularly concerned that:

1. The algorithmic scoring system under the draft RTS on the assessment of the inherent and residual risk profile of obliged entities (“RTS 1”) may assign disproportionately high inherent risk scores to CASPs based on an ill-fitting system and sectoral assumptions, and the final resulting residual risk score may not sufficiently reflect the strength of firms’ AML/CFT controls. This creates a risk of structurally inflated risk classifications, even for well-controlled entities, in a manner inconsistent with the EU’s risk-based supervisory principles;
2. The materiality thresholds under the draft RTS on the risk assessment for the purpose of selection of credit institutions, financial institutions and groups of credit and financial institutions for direct supervision (“RTS 2”) are too low and too vague to serve as an appropriate basis for eligibility criteria for direct AMLA supervision;
3. The RTS on Customer Due Diligence (“RTS 3”) requirements introduce burdens that may exceed current national rules and are inconsistent with the crypto-specific provisions crafted in the Transfer of Funds Regulation as the EU’s implementation of the FATF Travel Rule, without clear justification or transition;
4. The enforcement regime under the draft RTS on pecuniary sanctions, administrative measures and periodic penalty payments (“RTS 4”) requires further procedural and risk-based safeguards.

In the following commentary, we elaborate further on our key concerns and suggest potential improvements for EBA’s consideration.

I. Over-reliance on Inflexible and Inadequate Risk Scoring Methodologies

We commend efforts by the EBA to introduce standardized risk assessments. However, we are concerned that the algorithmic scoring model may not account for the operational diversity of the financial ecosystem. In particular, crypto business models differ significantly in terms of size, jurisdictional exposure, and the nature of client engagement.

Many inherent risk indicators outlined in the draft RTS are either ill-suited for or inappropriately targeting CASPs - e.g., customer residency tracking, use of unhosted wallets, or reliance on remote onboarding. While RTS 1 identifies over 200 data points, it is unclear which are mandatory, optional, or sector-specific. Nor is it clear how these points will be weighted, or how supervisory authorities may adjust final risk ratings. While we understand that many data points may not be applicable to CASPs - and thus would not be included in a CASP risk assessment - it remains unclear as to whether the divergence in applicability of risk factors might create an uneven playing field, also given that weighting is not (yet?) specified.

We believe there are legitimate concerns regarding suitability for comparison purposes, as well as the concern that it may be significantly more likely for CASPs to land in default “high-risk” classifications, which may distort supervisory intensity and lead to over-inclusion under AMLA’s direct oversight framework (see below). For example, data points such as the “total amount (EUR) hosted on the custodian wallets” or the “total number of transactions crypto-fiat” in various iterations are integral features of CASP business models and not inherently indicative of elevated ML/TF risk, but may be weighted heavily in the absence of context. In fact, the data points applicable to CASPs seem excessive. Without additional qualitative interpretation or thresholds, such indicators could result in inflated risk scores and increased supervisory burden for otherwise low-risk entities.

Therefore, we suggest that EBA consider:

- Tailoring the risk score algorithm to clearly defined subcategories by sector, business model, and operational scale.
- Explicitly recognizing crypto-native controls (e.g., blockchain analytics, smart contract audits) as risk mitigants.
- Clarifying which data points are required for everyone and how weighting, supervisory judgment and comparison will be applied in practice in order to ensure a sufficient basis for comparison that does not compare apples to oranges.

II. Risk of Over-inclusive Direct Supervision by AMLA

We are concerned that the thresholds for triggering AMLA supervision (i.e., operating in six or more Member States + high residual risk + 20,000 customers or €50M annual transaction volume) are not appropriately calibrated - especially for the crypto sector. These figures may capture a large number of CASPs, likely significantly more than the target numbers for direct AMLA supervision, and risk including firms with strong controls, and that pose no systemic risk. As noted in our general comments above, we believe that an overinclusion of CASPs will go against the AML level 1 mandate and political intention of focusing AMLA’s limited resources on those cross-border entities where the quantum of risk is greatest - i.e. most likely in the traditional banking sector.

The RTS does not clearly define what constitutes “operating in a Member State.” We do not believe that this definition can be used in the same way for systemically significant operators, such as cross-border investment banks, as for CASPs, given the very different levels of risk exposure as well as quantum of activity. Additionally, CASPs may be deemed to be operating passively (e.g., servicing customers remotely without licensing) or based on wallet activity, raising uncertainty. Moreover, the transaction volume and customer thresholds may over-emphasize scale rather than systemic risk.

More particularly, we are concerned that:

- The residual risk scoring criteria are opaque;
- The thresholds may capture firms simply due to a few large users (“whales”), or due to a high number of small transactions which has a higher likelihood to occur for CASPs due to financial inclusion in the crypto sector and accessibility of services;
- The customer criterion seems to include registrants who have never actually undertaken a transaction, or only one-time users, which is not reflective of systemic importance;
- There is no mechanism to challenge supervisory designation or account for changes over time.

Thus, we recommend (1) clarifying what constitutes “operating” in a Member State, particularly for digital-only models or passporting models under MiCA; (2) reassessing the materiality thresholds and definitions to ensure they reflect systemic risk, not merely customer count or activity volume; and (3) establishing a review mechanism or safe harbor process for edge cases. Finally, we suggest considering providing guidance on what happens when thresholds are crossed temporarily, or only in one of two years, potentially drawing on experience from the Single Supervisory Mechanism when it comes to EU supervision of banks in order to avoid a process whereby firms might regularly fall in/out of the systemic category.

III. Customer Due Diligence Standards May Undermine Technological Neutrality

CCI welcomes the goal of a harmonized EU-wide CDD standard. A single standard applicable across all Member States would be a significant step forward in reducing regulatory fragmentation and compliance inefficiencies. However, as drafted, the RTS 3 raises several legal and operational concerns — particularly for CASPs that operate cross-border and rely on digital onboarding tools.

Our concerns fall into three main categories:

1. Legal clarity on national laws and transition

The RTS does not clarify whether it overrides national requirements (such as specific heightened obligations in Ireland or Austria), or whether national rules may continue to apply in parallel. If national CDD provisions remain in force after the AMLR and RTS take effect, this would defeat

the harmonization objective of the AML package. For example, Members have flagged ongoing challenges with jurisdiction-specific “gold-plating” under AMLD5, including documentary PoA requirements that significantly impair onboarding efficiency without clear AML benefit. It is critical to confirm that the RTS sets a binding and exclusive standard — or, at a minimum, whether national supervisors may continue to impose stricter requirements after the RTS enters into force.

Additionally, many CASPs have invested significant resources in aligning with existing EBA Guidelines regarding CDD (e.g. EBA/GL/2021/02; EBA/GL/2024/01) that were also used as a basis for these RTS, and the interplay between the RTS and these guidelines, as well as the anticipated effect on any Member State guidance notes building on them, appears unclear.

2. Outdated or impractical documentation standards

The extensive list of minimum information required under Article 5 (e.g. place of birth, nationality, proof of address) may render many legitimate ID documents (such as driver’s licenses) unusable for CDD purposes. This approach risks excluding vast customer segments from access to compliant services. Moreover, fallback provisions for identity verification still require data points that are not always relevant or reliably available, particularly for mobile-only users, migrants, or younger adults. The RTS should recognize that the goal of CDD is to enable a reasonable, risk-based identification — not to verify every informational field printed on an identity document. This principle, already acknowledged by other regulators such as FinCEN in the U.S., should be explicitly endorsed by the EBA.

3. Overly restrictive interpretation of onboarding

Article 6 seems to make live video biometric checks the de facto standard for remote onboarding, excluding valid risk-based methods such as document scans, selfie verification, or NFC-based checks. Biometric data, while useful in some contexts, also carries heightened data protection risks due to its permanence and sensitivity, and may not be the most secure or appropriate solution for all business models. Entities should retain discretion to implement secure and proportionate identity verification tools based on risk exposure and technological capability.

We therefore recommend (1) clarifying that the RTS 3 sets a maximum standard and precludes national divergence in AML (CDD) requirements once in force; (2) adopting a technology-neutral standard for identity verification, allowing a range of risk-based onboarding methods on par with technological possibilities. We also encourage the EBA to ensure that minimum information requirements under Article 5 do not inadvertently preclude the future use of decentralized identity solutions. These systems can offer privacy-preserving, secure, and verifiable attestations without centralized storage of sensitive data. As these frameworks evolve, they may provide compliant identity verification while enhancing user control and data minimization, consistent with EU data protection objectives. We recommend that the RTS maintains future compatibility by remaining agnostic to the underlying identity architecture.

Additionally, we request that EBA provides a reasonable (at least twelve-months) grace period for implementation and clarify transition periods for legacy customers.

IV. Enforcement Framework Requires Greater Proportionality and Clarity

We support the move towards harmonized and consistent enforcement across the EU. However, the RTS as drafted leaves open several concerns:

- The use of periodic penalty payments and classification of “systemic breaches” is not clearly linked to actual risk or harm.
- The RTS does not provide clarity on due process protections or mechanisms to challenge enforcement measures.
- CASPs with innovative models may be unfairly penalized through being more likely to fall outside traditional expectations and face excessive scrutiny.

We urge EBA to advise implementing authorities to ensure that classification of breaches is proportionate to actual risk and not based on novelty or regulatory misalignment.

Additionally, we suggest considering including good-faith exceptions or risk-based exemptions for entities that are proactively engaging with regulators and actively investing in risk mitigation techniques such as blockchain/data analytics.

V. Further Recommendations

We urge the EBA/AMLA to develop a sector-specific annex or interpretive guidance clarifying the application of these RTSs to CASPs. Given the fast-moving nature of the sector, we also strongly recommend that a “digital assets stakeholder advisory group” be created for innovative business models, to complement the existing banking stakeholder group and enable regular dialogue between public authorities and private sector/market experts.

Finally, we ask for further clarity regarding the application of various existing EBA guidance (NCA-facing and private sector-facing) in this space. The RTSs should clearly map the interplay (or stipulate the expiration, keeping in mind the myriad of sources private and public sector participants alike already are and will need to be taking into account) of any existing guidelines with these future AML package-related workstreams, including these RTSs, to allow for continuity/consistency, feasibility and proportionality in implementation as well as administrative burden reduction, as espoused by the EU institutions’ current political intentions.

* * *

CCI appreciates the EBA’s leadership in this transitional phase and the opportunity to engage constructively at this early stage of implementation of the EU’s new AML/CFT regime. The draft RTSs will shape how AMLA and Member State authorities supervise CASPs and other

entities for years to come. It is essential that the framework remain risk-based, proportionate, and technology-neutral. CCI would welcome the opportunity for continued engagement with the EBA/AMLA on the further refinement of these important standards. We and our members are at your disposal for a follow-up meeting to discuss some of the issues raised in this consultation response, should that be useful to you as you develop your initial thinking on these RTSs.

Respectfully submitted,

Crypto Council for Innovation