coinbase

To:
The Anti-Money Laundering Authority

MesseTurm
Friedrich-Ebert-Anlage
49 60308
Frankfurt am Main
Germany

Submitted via AMLA's Consultation Page

8 May 2026

Re: Response to Consultation on Draft Regulatory Technical Standards under Article 28(1) of Regulation (EU) 2024/1624 (Customer Due Diligence Requirements) and Draft Regulatory Technical Standards under Article 19(9) of Regulation (EU) 2024/1624 (Business Relationships and Occasional Transactions)

Dear Sir/Madam,

Coinbase welcomes the opportunity to respond to the consultation on the draft Regulatory Technical Standards ("**RTS**") on Customer Due Diligence ("**CDD**") requirements under Article 28(1) of the Anti-Money Laundering Regulation (Regulation (EU) 2024/1624) ("**AMLR**"), and the draft RTS on Business Relationships and Occasional Transactions under Article 19(9) of the AMLR.

Coinbase is a leading global crypto-asset service provider ("**CASP**") authorised and regulated in multiple EU Member States, including Ireland and Luxembourg, as well as in the United Kingdom and other jurisdictions. We are committed to maintaining the highest standards of AML/CFT compliance and support **AMLA**'s objective of establishing a harmonised, risk-based framework for CDD across the EU.

We set out below in the Appendix our comments on specific articles of the draft RTS where we believe clarification, amendment, or reconsideration would strengthen the proportionality, effectiveness, and practical operability. Our comments are informed by our experience as a digital-first, non-face-to-face financial services provider operating at scale across the EU.

Yours sincerely,

Scott Bauguess, Vice President, Global Regulatory Policy, Coinbase

Appendix

1. Comments on the draft RTS on Customer Due Diligence

1.1 General Observations

We broadly support the risk-based approach affirmed in Article 1 of the draft RTS and the principle that the extent and nature of CDD measures should be commensurate with the type and level of risk identified. However, we note that several provisions in the draft RTS appear to depart from this principle by imposing prescriptive, one-size-fits-all requirements that may not be proportionate to the risk presented, particularly in the context of digital onboarding and crypto-asset services. We urge AMLA to ensure that the final RTS consistently reflects a risk-based approach throughout.

1.2 Article 4 — Specification on the Provision of the Place of Birth

Concern: Article 4 requires obliged entities to collect at least the country name as the place of birth, and any additional place of birth information contained on the identity document.

Comment: We question the proportionality and risk-mitigation value of requiring the collection of place of birth as a mandatory CDD data point. This requirement is not standard practice in many jurisdictions and it is unclear what specific ML/TF risk this data element is intended to identify or mitigate. Collection of place of birth (beyond country) would be unnecessary to achieve the purpose of Article 22(1)(a)(ii), as country of birth would be sufficient, and in the majority of cases, provides no additional useful information to the obliged entity to evaluate the AML/CTF risk.

Further, if additional detail on place of birth is required, this would create significant operational costs, particularly in respect of pre-existing customers, as this information will need to be collected and captured as part of future customer CDD refresh.

While we acknowledge that place of birth may serve as an additional data point for sanctions and PEP screening (and indeed may assist in confirming or disproving screening matches) the mandatory nature of this requirement across all risk levels appears disproportionate.

Recommendation: If this requirement is retained, we request confirmation that "place of birth" refers to the country of birth only. The collection of more granular information (e.g. city or region) should not be mandated; although may be collected where available in line with a risk-based approach.

1.3 Article 5 — Specification on Nationalities

Concern: Article 5 requires obliged entities to obtain information on all nationalities or, where applicable, the statelessness and refugee or subsidiary protection status, of the customer, any natural person purporting to act on behalf of the customer, and the natural persons on whose behalf, or for the benefit of whom a transaction, or activity is being conducted.

Comment: The requirement under Article 5 of the draft RTS (in line with Article 22(1)(a) of the AMLR) requires the collection of information on all nationalities (or other status). Our understanding of the purpose of this requirement is to help regulated entities assess the potential money laundering and sanctions risk of a customer (e.g. a customer who is a national of a high risk or sanctioned country), not to further verify their identity. Therefore, please confirm the wording of “obtain” requires collection but not verification of all nationalities collected, as that has been the standard process in Europe and any deviation would be overly burdensome.

We separately seek clarification on the practical application of the requirement to obtain nationality (or other) status on “the natural persons on whose behalf or for the benefit of whom a transaction or activity is being conducted” in the context of intermediary or pooled account structures, as the obliged entity does not have a customer relationship with or direct access to the underlying end user. It may therefore be practically difficult, and would in our view be disproportionate and overly burdensome, to collect all nationalities for underlying these end users and ask that this scenario be clarified.

We also query how obliged entities are expected to identify and collect information on the "statelessness and refugee or subsidiary protection status" of a customer in practice. This information is not typically disclosed voluntarily and may not appear on identity documents. Guidance on the expected means of collection and the consequences of an inability to obtain this information would be welcomed.

Recommendation: AMLA should confirm whether verification of all nationalities is required, should provide practical guidance on the means by which statelessness and

protection status are to be identified and collected, and should clarify the application of this requirement in intermediary and pooled account contexts.

1.4 Article 6 — Documents for the Verification of Identity

Concern: Article 6(5) requires obliged entities to obtain the identity document, passport or equivalent, or a certified copy thereof, or act in accordance with Article 7 on non-face-to-face verification measures. Article 6(6) provides that electronic identification means *"shall be permitted to verify the identity of the natural person in a face-to-face context".*

Comment: We have a number of comments in connection with this article:

(a) Sufficiency of digital copies: In our view, a digital copy (*e.g.* a scanned image or PDF) of an identity document, when verified in accordance with the remote verification measures set out in Article 7 (including liveness checks and document authenticity verification) should be sufficient to satisfy the requirements of Article 6. The requirement for a "certified copy" should not be interpreted as requiring physical certification or notarisation, which would be incompatible with digital-first onboarding processes and would undermine the EU's broader digital strategy. For digital onboarding, physical certification or notarisation of original documents provides limited value in terms of verification of the digital document's veracity. Such veracity checks for digital documents are, and can be, undertaken irrespective of any certification or notarisation, having regard to the digital copy of the document submitted, and the information contained therein.

(b) Electronic identification in non-face-to-face contexts: Article 6(6) appears to limit the use of electronic identification means (as described in Article 7(1)) to face-to-face contexts only. This is a significant concern. The regulation should expressly permit the use of electronic identification means (including eIDAS-compliant electronic identification schemes) for the verification of identity in non-face-to-face contexts, without the mandatory collection of a physical identity document. Restricting electronic identification to face-to-face settings is inconsistent with the objectives of eIDAS 2.0 and the European Digital Identity framework, and would create an unjustified barrier to digital onboarding.

(c) Definition of an "identity document": The phrase "equivalent to an identity document or passport" implies that an "identity document" and "passport" will automatically be deemed a sufficient verifying document, even if they do not

have all of the features set forth in Article 6. If that is the intent (which we agree it should be to satisfy Article 22(6) of the AMLR), then:

- this should be clarified beyond a doubt in the RTS; and
- the term "identity document" should be defined to clarify that they are a category of documents other than identity documents or passports (as no definition of either term is currently provided for in either the AMLR or the RTS).

For example, we would propose that national identification cards, government issued driver's licences, VISAs, residence permits, public service cards used for social welfare entitlements, government issued health cards, documentation in relation to refugees and asylum seekers and other similar government issued documents should fall under the definition of an *"identity document"* that by default is acceptable, even if it does not contain all of the features set forth in Article 6. The conditions set forth in Article 6 would then apply to other identification documents that do not qualify as a "passport" or "identity document".

(d) Requirement to meet all prerequisites under Article 6: For documents that do not qualify as an "identity document" or "passport", it is unreasonable to demand that all of the conditions set forth in Article 6 of the RTS be satisfied before deeming the identification document as reliable. Instead, a risk-based approach, having regard to the nature of the documents, and the reasons for its submission as an alternative to an identity document or passport, should be permitted. We would note this for the following reasons:

- Verification of the identity of the customer has historically meant that obliged entities must obtain enough reliable information to assure themselves that the person is who they claim to be. It does not mean they need to verify every data point collected from the applicant (i.e. name, date of birth, address, etc.). This concept has been adopted by other FATF-regulated countries with equivalent AML/CTF Regimes. As such, not every data element collected from the customer must appear on the verifying identification document collected.
- Recital 7 of the draft RTS acknowledges that there may be situations where identity documents issued to or held by the customer do not meet the attributes of an identity card or passport, such as where the customer is an asylum seeker. To mitigate the risk of financial exclusion and unwarranted derisking, the criteria laid down in the draft RTS concerning identification documents should be applied in a way that takes into

account the reason why a legitimate customer may be unable to provide standard documentation. This is in line with previous statements made by the EBA in its Opinion on 'de risking' (EBA/Op/2022/01) and also its Statement on Financial Inclusion in the context of the Invasion of Ukraine (published 27 April 2022).

- It will be incredibly rare for other forms of reliable identification documents across the EU and beyond to contain all of these characteristics set out in Article 6 of the RTS. For example, not all identification documents have signatures on them.
- The term "legitimate reasons" is subjective and would require obliged entities to document: a) initial attempts to obtain an equivalent identification document; b) a "legitimate reason" provided by the customer as to why they cannot provide such an equivalent document. This would potentially add operational costs to obliged entities and either delay the onboarding process or, at worse, cause these applicants to be rejected and force them to engage in underground banking, which would be outside the scope of monitoring by regulated financial institutions and law enforcement (contrary to the overall policy intent of the AMLR).

Recommendation: We recommend that the draft RTS be updated to:

- Confirm that digital copies of identity documents, verified through compliant remote solutions under Article 7, satisfy the requirements of Article 6;
- Clarify that "certification" does not require physical or formal notarisation of documentation;
- Amend Article 6(6) to expressly permit the use of electronic identification means in non-face-to-face contexts;
- Ensure that the RTS does not create a hierarchy that subordinates electronic identification to physical document collection, given the EU's commitment to digital identity;
- Provide a clear definition of an "identity document"; and
- Allow for a risk-based approach to the use of documents other than identity documents or passports on a risk-based approach.

1.5 Article 7 — Verification Measures Conducted on a Non-Face-to-Face Basis

Concern: Article 7(1) requires obliged entities to use electronic identification means meeting the "substantial" or "high" assurance levels under Regulation (EU) No 910/2014 (eIDAS) for non-face-to-face verification. Article 7(2) provides that where such solutions are *"not available, or cannot reasonably be expected to be provided"*, obliged entities may use remote solutions meeting the safeguards in paragraphs 3 and 4.

Comment: We support the safeguards set out in Article 7(3), which align with industry best practice for remote identity verification (including liveness checks, document authenticity controls, and secure data retention). Our current onboarding processes for EU customers already incorporate identity document verification combined with biometric selfie matching, which we believe meets or exceeds these requirements.

However, we reiterate the concern raised under Article 6, namely that the RTS should confirm that a digital copy or image of an identity document, verified through compliant remote solutions (including liveness and document authenticity checks), is sufficient, and that no additional physical certification or original document collection is required.

We also note that eIDAS-compliant electronic identification schemes at the "substantial" or "high" assurance level are currently available in only a limited number of Member States (*e.g.* Germany, Italy, Croatia, Estonia, Spain, and Luxembourg). For customers presenting identity documents from other jurisdictions, the fallback to Article 7(2)–(4) will be the norm rather than the exception. The RTS should acknowledge this reality and ensure that the fallback provisions are treated as a fully equivalent verification pathway, not as a secondary or inferior alternative.

There are many other reliable biometric screening tools available that permit obliged entities to confidently verify a remotely onboarded customer’s identity. Such tools are currently offered by reputable vendors and are presently being used by many sophisticated financial institutions. In our view, these solutions provide the same level of protection as eIDAS solutions. While eIDAS creates a framework for electronic identification, it does not contain additional liveness controls that can mitigate fraud attempts. In our experience, such liveness checks are arguably a stronger mitigant against identity fraud, as they represent biometric techniques to verify the applicant is: a) a real/live person; b) in possession of a valid ID document (not a spoofed one); and c) is who they are claiming to be. We therefore believe that an approach reflecting a technologically neutral approach should be adopted; avoiding a hierarchy of remote onboarding solutions.

Recommendation: Confirm that digital copies verified through compliant remote solutions are sufficient; ensure parity of treatment between eIDAS-based verification and remote verification solutions meeting the Article 7(3) safeguards.

1.6 Article 11 — Understanding the Ownership and Control Structure of the Customer

Concern: Article 11 requires obliged entities to take risk-sensitive measures to understand the ownership and control structure of the customer, including assessing whether there is an *"economic, legal or other rationale behind the structure".*

Comment: While we support the objective of understanding ownership structures, the nature and extent of inquiry and assessment of the *"economic, legal or other rationale"* behind a group structure, as drafted, is unclear, and potentially disproportionate and burdensome. In particular, obliged entities should not be required to undertake legal analysis of customer group structures. Such a requirement would be prohibitively expensive, and would not, in our view, be appropriate or proportionate, particularly for lower risk customers. This requirement should only extend to high risk customers.

We note that Article 12 of the draft RTS already provides specific, enhanced measures for complex corporate structures (defined as structures with three or more layers between the customer and the beneficial owner, plus additional complexity indicators). The requirement to assess the rationale behind a structure should be linked to the higher-risk, complex structures addressed in Article 12, rather than applied as a blanket obligation for all group structures.

Recommendation: Clarify that the obligation to assess the economic, legal, or other rationale behind a group structure applies specifically to complex corporate structures as defined in Article 12, or to structures that present elevated ML/TF risk indicators, rather than to all corporate customers.

1.7 Article 12 — Understanding the Ownership and Control Structure in the Case of Complex Corporate Structures

Concern: Article 12(1)(b) provides that one of the conditions for treating a structure as *"complex"* is that *"the customer and any legal entities present at any of these layers are registered in jurisdictions outside the EU".*

Comment: Whilst it is recognised that greater scrutiny should be placed on complex ownership structures, in our view the mere inclusion of a non-EU entity in any layer of an ownership structure should, of itself and without more, be treated as an inherent indicator of complexity and automatically trigger enhanced due diligence. Many legitimate, low-risk, corporate groups include entities incorporated in well-regulated third countries with AML/CFT frameworks equivalent to or no less robust than those of the EU (*e.g.* the United Kingdom, Switzerland, Singapore, the United States, amongst others). Treating the presence of any non-EU entity as an automatic complexity indicator is inconsistent with a risk-based approach and could result in a disproportionate compliance burden for obliged entities servicing international corporate clients.

Recommendation: This condition should be refined to refer to entities registered in third countries that have been designated as high-risk by the EU. This would ensure that the complexity indicator is genuinely risk-based and does not capture legitimate structures involving well-regulated jurisdictions.

1.8 Article 16 — Identification and Verification of the Person Purporting to Act on Behalf of the Customer

Concern: Article 16 requires obliged entities to obtain information enabling them to verify the *"existence and extent of the power of representation"* of any person purporting to act on behalf of the customer.

Comment: We welcome this requirement in principle but note that the term *"person purporting to act on behalf of the customer"* is not clearly defined in the draft RTS. We note that in the UK, HM Treasury has clarified that the equivalent terms in the UK refers to entities acting on behalf of individuals or third parties acting on behalf of an organisation (*e.g.* intermediaries, legal agents, persons with a power of attorney), and is not intended to capture employees of the corporate customer, for example who have the authority to submit trade instructions on the corporate customer's behalf (*e.g.* authorised signors).

We support this approach and recommend it be adopted here for the following reasons:

- Employees of corporate customers do not represent the same ML/TF risks as the corporate customer itself or its beneficial owners, as they do not directly benefit from the provided services;

- Furthermore, these employees have already been screened (e.g. background checks) by the corporate customer, further reducing any risk;
- It is also quite common for corporate customers to present lists of authorised signors who have authority to instruct on an account that contain dozens and, in instances of larger financial institutions, hundreds of individuals, therefore requiring regulated entities to perform full CDD on, and “verify the existence” of, all such persons would be disproportionate and operationally overburdensome without delivering meaningful AML/CFT risk mitigation.

This is not to say that obliged entities would not, in practice, apply anti-fraud controls or checks to such employees / authorised signors as part of their policies and procedures. However, such anti-fraud measures should be applied on a risk-based approach, and not incorporated as a requirement into the obliged entity’s AML/CFT systems and controls.

Recommendation: AMLA should provide a clear definition of *"person purporting to act on behalf of the customer".* This should clarify that this does not include employees of corporate customers who may operationally interact with the obliged entity (*e.g.* authorised signors), but should only include third parties acting on behalf of the customer (*e.g.* intermediaries, persons with a power of attorney).

1.9 Article 20 — Minimum Requirement for Customer Identification in Situations of Low Risk

Concern: Article 20(1)(a)(ii) requires the collection of *"place of birth"* even in situations of low risk.

Comment: Consistent with our comments on Article 4 above, we request confirmation that *"place of birth"* in the context of low-risk simplified due diligence refers to the country of birth only, and does not require more granular information (*e.g.* city, region, or state) unless such information appears on the identity document presented.

Recommendation: Confirm that *"place of birth"* means country of birth for the purposes of Article 20.

1.10 Article 22 — Sectoral Simplified Measures with Respect to Pooled Accounts

Concern: Article 22 provides simplified CDD measures for credit institutions that open pooled accounts (*i.e.* accounts in which the account holder administers the funds of its clients). As currently drafted, the provision is limited in scope to only credit institutions.

Comment: We note that pooled account structures are not unique to credit institutions. Other regulated financial service providers (including investment firms, CASPs, electronic money institutions ("**EMIs**"), and payment institutions ("**PIs**")) may also operate pooled or omnibus account structures in which they hold, administer or custody funds or assets on behalf of their clients.

The rationale for the simplified measures in Article 22 (namely, that the account holder is itself an obliged entity subject to AML/CFT obligations and effective supervision, and that the ML/TF risk is low) equally applies to pooled accounts held by these other categories of regulated entities. This provision therefore should not be limited to credit institutions, and should apply to all financial institutions.

We also query whether, in the absence of an express provision covering pooled accounts held by non-credit institution obliged entities, such arrangements would instead be categorised as correspondent relationships (as is currently the case for accounts provided to PIs/EMIs by credit institutions under certain national frameworks). If so, this would result in disproportionately burdensome enhanced due diligence requirements for arrangements that present comparable risk profiles to those covered by Article 22.

Recommendation: Article 22 should be expanded to cover pooled accounts operated by all categories of financial institution obliged entities, including investment firms, CASPs, EMIs, and PIs, provided that the conditions set out in Article 22(a)–(e) are met. Alternatively, AMLA should clarify the CDD treatment applicable to pooled accounts held by non-credit institution obliged entities.

1.11 Article 29 — Screening of Customers and Beneficial Owners

Concern: Article 29 requires obliged entities to establish whether customers, beneficial owners, and controlling/owning entities are subject to targeted financial sanctions. It further provides that *"where there is a suspicion of circumvention or evasion of targeted*

financial sanctions" obliged entities must also establish whether the person acting on behalf of the customer is subject to targeted financial sanctions.

Comment: We welcome the distinction drawn in Article 29 between the mandatory screening of customers, beneficial owners, and controlling entities on the one hand, and the conditional screening of persons acting on behalf of the customer where there is a suspicion of circumvention or evasion on the other. This is a proportionate and risk-based approach.

We request confirmation that this distinction is intentional and that obliged entities are not required to routinely screen all persons acting on behalf of the customer against targeted financial sanctions lists in the absence of a suspicion of circumvention or evasion.

Recommendation: Confirm that the screening of persons acting on behalf of the customer

1.12 Annex I — Attributes for Electronic Identification

Concern: Annex I defines the corresponding list of attributes that electronic identification means and qualified trust services are required to feature for the purpose of applying CDD. These are based on Commission Implementing Regulation (EU) 2024/2977 which lays downs rules on European Digital Identity Wallets.

Comment: In terms of the list of attributes set out in Annex I, minor clarification should be provided to confirm that country of birth is sufficient for natural persons, and that the distinction between country and state entries is only applicable where relevant (as not all Member States have federal sub-divisions).

Recommendation: Clarify that country of birth is sufficient, and that a distinction between country and state entries is only applicable where relevant.

2. Comments on the draft RTS on Business Relationships and Occasional Transactions

2.1 General Observations

We broadly support the objective of establishing clear, harmonised criteria for distinguishing business relationships from occasional transactions, and for identifying linked transactions. These are fundamental concepts underpinning the application of CDD obligations, and consistency across the EU is essential for both effective AML/CFT compliance, a level playing field for obliged entities, and the proper functioning of the Single Market.

However, we note that certain provisions in the draft RTS, particularly as they apply to digital-first service providers and CASPs, risk creating outcomes that are disproportionate to the ML/TF risks presented, or that are operationally impracticable in the context of modern digital service delivery. We urge AMLA to ensure that the final RTS reflects the realities of digital onboarding and service provision, and avoids conflating technical access to a platform with the establishment of a substantive financial services relationship.

2.2 Article 2 — Criteria for Distinguishing a Business Relationship from an Occasional Transaction

Concern: Article 2(1) provides that obliged entities shall, for the purpose of distinguishing a business relationship from an occasional transaction, "*at least take into account the use of online services through a registration providing ongoing access as a criterion when considering the element of duration included in the definition of a business relationship."*

This provision appears to treat the mere act of registering for an online account as, of itself, a sufficient indicator of the *"duration"* element of a business relationship. In the context of digital-first financial services, and CASPs in particular, this interpretation would have significant and potentially unintended consequences.

Comment: We acknowledge that Recital (5) of the draft RTS confirms that business relationships and occasional transactions are mutually exclusive, and that a business relationship requires an element of *"repetition or duration"* as defined in the AMLR. The example given is that of a one-off donation through a crowdfunding intermediary.

Recital (7) of the draft RTS emphasises that a business relationship requires the expectation, or subsequent acquisition of, an element of during. In respect of online services through a registration providing ongoing access should be taken into account when considering this element, and that *"[n]ormally and by its nature, the use of online services after having gone through any form of registration implies that a certain degree of duration of the provision of services may reasonably be expected."* This requirement is set out in Article 2(1), which states that obliged entities must at least take into account the use of online services through a registration providing ongoing access *"as a criterion when considering the element of duration"*. These provisions could be taken to imply that in almost all cases the simply act of online registration will imply duration and therefore automatically fall within the definition of a business relationship.

Notwithstanding, Article 2(3) makes specific reference to CASPs providing exchange of fiat-for-crypto, crypto-for-crypto, and crypto-transfer services (as well as currency exchange and payment services) in the context of linked transactions. Carrying out at least 3 or more transactions within a rolling period of 12 months is set as a criterion when considering the element of repetition. Occasional transactions are therefore contemplated in the context of crypto-asset (and other) services (both under the draft RTS and in Article 19(2) of the AMLR when under €1,000). We would be supportive of the use of these criteria (3 transactions in 12 months) as general prerequisites for the establishment of a business relationship.

For the reasons set out below, we consider that the nature of the services, rather than the fact of online registration, should be the determining criterion. Thus, a linked transaction approach is more appropriate for determining whether a relationship with a customer will involve an element of repetition or duration where the service is potentially one-off in nature (*e.g.* crypto-transfer services). This can be contrast with services requiring an on-going or durable relationship (*e.g.* custody) where a business relationship is inevitable. The fact that both services are accessed through online registration should not be determinative of the regulatory treatment. Whilst this is somewhat recognised in Article 2(3), it is otherwise unmined by Article 2(1), as well as Recital (7), which imply that registration is potentially sufficient without more to evidence duration of relationship.

Specifically in the context of crypto-asset services, we would note that in order to receive any crypto-asset service, given their online nature, it will be necessary in the first instance to register with the provider. However, in our experience, a significant proportion of users who register for a CASP's platform do not proceed to conduct any regulated financial transaction, or may do so on only a once off basis. For example:

- *Users who register but are not approved for trading:* Many users create an account but do not complete the onboarding process or are not approved for trade-eligible status. Their access to the platform may be limited to viewing publicly available market data (*e.g.* crypto-asset prices, market capitalisation data, and educational content). These users have not entered into a relationship involving the provision of regulated financial services.
- *Users who register and conduct one or two, low-value transactions:* Some users may register, complete only one or two transactions, and never return to the platform. Treating such users as having established a *"business relationship"* solely by virtue of their registration, rather than by reference to the nature, frequency, or value of their activity, potentially conflates technical platform access with a substantive and on-going financial services relationship.
- *Inconsistency with the occasional transaction concept for CASPs:* If registration alone is determinative of a business relationship, it is difficult to see how a CASP could ever have an *"occasional transaction"* relationship with a customer, since virtually all CASP services are delivered through online platforms requiring registration. This would render the occasional transaction concept (and the associated CDD thresholds in Article 19 of the AMLR) effectively inapplicable to CASPs (as well as all other online services), which we do not believe is the intended outcome.

The general digitalisation of services means that registration for an online account is increasingly a prerequisite for accessing any service, including services that may be used only once or very infrequently. This could include crypto-asset services, payment services, and currency exchange, as well as crowdfunding services (which are used as the example in Recital (5)).

Treating registration as automatically establishing a business relationship fails to distinguish between:

(a) A genuine, ongoing relationship involving the repeated or continuous provision of regulated financial services (either by virtue of the nature of the service which requires an ongoing relationship, or through repeated transactions); and

(b) A one-off or incidental use of a digital platform that happens to require account creation for technical or security reasons.

Recommendation: Article 2(1), as well as the Recitals, should be amended to clarify that registration for an online account, of itself, does not automatically establish a business relationship. Instead, registration should only trigger a business relationship where it is intrinsically linked to the provision of an ongoing or durable regulated services or

financial transactions, *i.e.* where the registration provides ongoing access to regulated financial services that the customer has activated or utilised, rather than mere access to a platform or informational content. The use of 3 transactions in a 12 month period as a general prerequisite to the establishment of an online business relationship would be helpful in providing proportionality and clarity in this context.

These amendments should confirm that:

- The nature of the services should be determinative of whether there is a business relationship or an occasional transaction;
- The means of access to a services should not be determinative of whether there is a business relationship;
- Registration through an online platform does not, of itself, constitute a business relationship;
- The "duration" criterion requires a substantive, ongoing engagement with regulated services, not merely the existence of a dormant or inactive account;
- Occasional transactions remain possible in the context of CASP services, notwithstanding the requirement for online registration;
- Where possible, due to the nature of the services, transaction thresholds over a prescribed period (see also our comments in section 2.3 below), are a better proxy to duration for the purposes of determining a business relationship.

2.3 Article 3(1) — Scope and Nature of Enquiry for Broader Linking Criteria

Concern: Article 3(1) sets out criteria for identifying linked transactions, including:

(a) Transactions performed or received by the same natural or legal person (considering identical or similar origin and destination);
(b) Broader criteria *"based on information available to the obliged entity"*, including where customers are (i) family members, (ii) business partners, (iii) operating in concert, (iv) subsidiaries or beneficial owners of the same parent undertaking, (v) using the same digital infrastructure, or (vi) using common intermediaries or service providers facilitating transactions;
(c) Transactions pertaining to the same purchase (considering identical or similar purpose);
(d) Other relevant characteristics, including common characteristics, transactions at different establishments or through agent networks, transactions within a loyalty programme, and dependent transactions; and
(e) Transactions performed within a short timeframe.

While the criteria in Article 3(1)(a) relate directly to the customer (origin, destination, or purpose), the broader criteria in Article 3(1)(b) (family members, business partners, acting in concert, same digital infrastructure, and common intermediaries) are qualified only by the phrase *"based on information available to the obliged entity".* The nature and extent of enquiry required of the obliged entity in respect of these broader factors is not clear.

Comment: We support the principle that linked transaction identification should be based on information reasonably available to the obliged entity, and we welcome the qualification *"based on information available".* However, without further guidance, there is a risk that this provision could be interpreted as requiring obliged entities to undertake proactive investigations or data-matching exercises to identify potential links between customers, for example, to determine whether two unrelated customers are family members, business partners, or *"operating in concert".*

For a CASP operating at scale with millions of retail customers, such proactive enquiries would be operationally impracticable and disproportionate to the ML/TF risk presented by the vast majority of retail transactions.

Further, there is a question around when customer(s) are subject to CDD obligations for linked transactions involving multiple natural or legal persons. Specifically, there is a question on whether CDD must be performed on all persons involved in the linked transactions, only the person conducting the transaction that causes the aggregate threshold to be exceeded, or the person behind the originating transaction. In the absence of such guidance, obliged entities face uncertainty as to the scope of their obligations in relation to these types of customers and transactions.

Recommendation: We request that AMLA and the RTS clarify that:

- The obligation to identify linked transactions under Article 3(1)(b) is limited to information that is already held by or readily apparent to the obliged entity in the ordinary course of its business and CDD processes;
- Obliged entities are not required to undertake proactive investigations, external data-matching, or enhanced enquiries solely for the purpose of identifying potential links between customers under this provision (unless otherwise required as a result of increased ML/TF risks);
- The obligation is one of reasonable awareness, not exhaustive detection; and
- The scope of CDD on individuals involved in linked transactions, where more than one individual is involved.

2.3 "Use of the Same Digital Infrastructure"

Concern: Article 3(1)(b)(v) identifies *"use of the same digital infrastructure"* as a criterion for identifying linked transactions when considering identical or similar origin and destination. The term *"digital infrastructure"* is not defined in the draft RTS and is potentially very broad and could encompass a number of different circumstances which may more or less identify transactions as potentially being linked. This could include:

- Use of the same IP address (which may be shared by multiple unrelated users on the same network, VPN, or public Wi-Fi);
- Use of the same device (which may be a shared or public device);
- Use of the same blockchain address or wallet (which would be a more meaningful indicator);
- Use of the same internet service provider;
- Use of the same software, application, or browser; or
- Use of the same cloud infrastructure or hosting provider.

Such a potentially broad interpretation is also supported by discussion papers at an EU level, such as those published by the European Commission, *"White Paper - How to master Europe's digital infrastructure needs?"*, the Body of European Regulators for Electronic Communications (BEREC), *"Union Preparedness Plan for Digital Infrastructures"*, and the proposed Digital Networks Act, which talk about digital infrastructure across the EU and at a Union level.

Comment: Many uses of the same *"digital infrastructure"* (if defined broadly) would not inherently imply a linked transaction. For example, multiple unrelated customers may share an IP address because they are on the same corporate network, university campus, or public Wi-Fi hotspot. Similarly, the use of the same internet service provider or browser is not indicative of any connection between transactions.

If this criterion is intended to capture situations where multiple customers are using the same device or the same blockchain wallet/address to conduct transactions (which would be a more meaningful indicator of potential structuring or linked activity) this should be stated expressly.

The term *"digital infrastructure"* is an ambiguous term without additional clarification. Taken broadly this criterion risks generating a very high volume of false positives,

particularly for digital-first service providers, and could impose a disproportionate operational burden without delivering meaningful AML/CFT risk mitigation.

Recommendation: We request that the RTS include one or more of the following clarifications:

- A clear definition of *"digital infrastructure"* (or the use of an alternative term) for the purposes of Article 3(1)(b)(v), specifying the types of shared digital resources that are intended to be captured (*e.g.* shared devices, shared blockchain addresses/wallets) and those that are not (*e.g.* shared IP addresses, shared ISPs, shared browsers);
- Confirm that the use of the same digital infrastructure is an indicator to be assessed in conjunction with other factors, and does not, of itself, establish that transactions are linked; and
- Acknowledge that in the context of digital-first services, many customers will inevitably share certain elements of digital infrastructure without any connection between their transactions.

2.4 Rolling One-Month Period for CASPs

Concern: Article 3(2) provides that CASPs providing exchange of fiat-for-crypto, crypto-for-crypto, and crypto-transfer services must, for the purpose of identifying linked transactions, *"at least take into account the criterion of a rolling period of one month"* when considering the element of a specific period included in the definition of linked transactions.

Comment: We note that the requirement in Article 3(2) applies the same rolling one-month period to CASPs as to currency exchange offices and money remittance providers. While we understand the rationale for aligning the treatment of these service categories, we would observe that the nature and frequency of crypto-asset transactions may differ materially from traditional currency exchange or remittance services. In particular:

- Crypto-asset transactions may be conducted with much higher frequency and in much smaller individual amounts than traditional currency exchange or remittance transactions;
- The one-month rolling period, combined with the broad linking criteria in Article 3(1), could result in a very large number of transactions being identified as

"linked" for active retail customers, even where there is no structuring or ML/TF risk; and
- The operational burden of monitoring and aggregating all transactions within a rolling one-month window, across all linking criteria, is significant.

Recommendation: We do not object to the one-month rolling period in principle, but request that AMLA confirm that:

- The one-month period is a default position, and that obliged entities still retain the discretion to apply shorter or longer periods on a risk-sensitive basis where appropriate;
- The identification of linked transactions within the one-month period does not automatically trigger CDD obligations, instead CDD should only be triggered where the aggregate value of linked transactions meets or exceeds the relevant thresholds set out in Article 19 of the AMLR; and
- Obliged entities are permitted to apply risk-based filters and thresholds to manage the volume of potential linked transaction alerts, consistent with the risk-based approach.

---

3. Conclusion

Coinbase is committed to working constructively with AMLA to ensure that the final RTS on CDD and on Business Relationships and Occasional Transactions are proportionate, effective, and operationally workable for all categories of obliged entities, including digital-first service providers and CASPs.

We believe that the amendments, clarifications, and recommendations proposed above would strengthen the risk-based approach, reduce the risk of disproportionate compliance burdens, and ensure that the final standards reflect the realities of modern digital financial services delivery.

We understand that supplementary factsheets and guidance may be developed to accompany the final RTS. We strongly encourage AMLA to publish sector-specific guidance addressing the application of the RTS to CASPs and digital-first financial service providers, including worked examples of how the business relationship, occasional transaction, and linked transaction concepts apply in the context of crypto-asset services delivered through online platforms.

We would welcome the opportunity to discuss these comments further with AMLA and to provide any additional information or technical input that may be helpful.