dutch banking association

CONSULTATION REACTION

Reaction of the Dutch Banking Association
Date: 6 June 2025

Introduction

The Dutch Banking Association (*Nederlandse Vereniging van Banken, NVB*) welcomes the opportunity to respond to the EBA consultation on the draft Regulatory Technical Standards (RTS) under the EU's new AML/CFT regime. We appreciate the EBA's ongoing efforts to enhance the effectiveness, consistency, and proportionality of the implementation of AML/CFT requirements across the EU.

Our response focuses primarily on the draft RTS under Article 28(1) AMLR on Customer Due Diligence (CDD). In this context, we provide detailed, article-by-article feedback, addressing most of the consultation questions raised by the EBA. Our input reflects both the practical experiences of Dutch banks and interpretative challenges. Particular attention is given to provisions where the draft RTS appears to move away from the risk-based spirit of the AMLR, towards a more prescriptive, rule-based approach, which we believe may hinder effective and proportionate AML/CFT compliance in execution and supervision.

In addition, we include more general remarks on the other three draft RTSs, those concerning the assessment of inherent and residual risk profiles, the selection criteria for direct supervision by AMLA, and pecuniary sanctions and administrative measures. Our comments focus on implementation challenges, including the need for transitional arrangements and clear data definitions, and the legal complexity that arises from overlapping administrative and criminal enforcement regimes, which may limit the intended harmonisation.

Important general remarks

We wish to highlight several elements that are central to our response.

- We strongly support the inclusion of the five-year grace period, which we understand extends for existing customers until 10 July 2032. This period provides essential time for obliged entities to properly update identification information for existing customers with the new requirements. While we are committed to implementing the new rules expeditiously and in a risk-based manner, this grace period is both necessary and welcome.

Gustav Mahlerplein 29-35
1082 MS Amsterdam
www.nvb.nl

- We urge the EBA to reaffirm the central role of the risk-based approach throughout the RTS on CDD. In our view, the current draft RTS leans too much towards a rule-based approach, which is not appropriate in the context of AML/CFT measures. This is especially the case where the RTS details specific CDD and EDD measures in a prescriptive manner, even though the AMLR allows for proportionality through terms such as “where necessary”. For example, Articles 15 and 16 on the purpose and nature of the business relationship are overly rigid and do not allow for risk-sensitive implementation.

- To enhance clarity and unambiguity we would like to call your attention to consistency in formulation and terminology (e.g., natural person/ customer/ UBO/ person purporting to act on behalf of the customer), both throughout the RTSs and in line with the EU AML-package.

- The EBA Risk Factors Guidelines, the EBA Guidelines on remote customer onboarding solutions and other related guidance should be formally repealed when the RTS on CDD enters into force. Their continued coexistence with this RTS would create legal uncertainty and conflicting obligations for obliged entities. Given the direct legal effect of the RTS under the AMLR, these guidelines are no longer appropriate or necessary and are to be (partly) withdrawn to ensure clarity for obliged entities.

We trust that our contribution will support the development of practical and proportionate RTSs that enhance effective AML/CFT outcomes while reducing unnecessary efforts.

We remain available for further dialogue and clarification.

Contact

Helène Erftemeijer
Sector Coordinator AML/CFT & Sanctions
M +31 651579171
E erftemeijer@nvb.nl

Reaction per RTS and consultation questions

A) Draft RTS under Article 28(1) of the AMLR on Customer Due Diligence

Question 1: Section 1: Information to be collected for identification and verification purposes

Do you agree with the proposals as set out in Section 1 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

NVB reaction

Several provisions in the draft RTS lack sufficient proportionality and risk-based nuance. Requirements such as collecting detailed data on intermediate entities in a structure for parties with whom there is no business relationship, extensive documentation obligations in non-face-to-face onboarding, precise information on addresses and country of birth or verification of all datapoints, without regard to the risks, impose a significant operational and cost burden for obliged entities and substantial unnecessary impact on customers and society.

If adopted as currently drafted, the lack of flexibility will lead to disproportionate compliance costs, unnecessary customer outreach, and delays in onboarding, with limited corresponding risk-mitigating effect. For your reference, in the Netherlands an estimated 35.9mln banking relations exist with natural persons and business customers, for which the additional datapoints need to be collected by banks. This number does not yet include UBOs, SMOs, representatives and persons purporting to act on behalf of the customer. Therefore, the collection of information requires a significant effort with serious impact for customers, obliged entities and society.

We recommend incorporating clearer references to the risk-based approach, allowing obliged entities to tailor measures to actual risk exposure. Without such clarification, implementation will involve disproportionate costs and operational challenges with limited to no added value for AML/CFT effectiveness. The below table lists our reaction and suggestions regarding the articles in Section 1, which includes reactions to the consultation questions 1 and 2.

Article	Consultation reaction
1 – Names of natural persons and legal entities	We interpret Article 1 to require collection of all full names and surnames and/or initials of middle names as shown on the identity document. If all names are not listed, we consider it sufficient that the customer provides them. This article specifically refers to the “the customer's full names and surnames. It raises the question whether this is intentionally limited to the customer instead of a natural person.

	For legal entities we consider it only relevant to collect the commercial name when it differs materially from the registered name. The article should clarify that in those cases only the main commercial name is required. We would like to emphasise that this RTS should be process and system agnostic instead of referring to a specific type as in: “Obliged entities shall ask the customer ...”.
2 – Information to be obtained in relation to addresses	We understand Article 2 to apply specifically to natural and legal persons as referred to in Article 22(1)(a) and (b) AMLR. It is unclear whether the same requirements apply to persons and entities mentioned under Article 22(1)(c) and (d), such as trustees or representatives of organisations with legal capacity. We recommend clarifying this in the RTS. We propose flexibility in situations where no postal code or street name exists. In such cases, obliged entities should be allowed to record the address as provided by the customer, consistent with Article 22(1)(a)(iv). We interpret “obtain” in this context to mean requesting the information from the customer, not verifying the address information.
3 – Specification on the provision of the place of birth	We assume that the reference to “country name” in Article 3 follows the same standard as outlined in Article 2 of the RTS, meaning either the full country name or the ISO 3166 alpha-2 or alpha-3 code. In practice, not all official identity documents include both the city and country of birth. We therefore propose that it should be sufficient to obtain at least one of these two data points, unless both are demonstrably required for risk mitigation purposes. Moreover, its use may raise concerns about potential discrimination.
4 – Specification on nationalities	We interpret the requirement to “satisfy themselves” that obliged entities must ask the customer to declare all nationalities held. We consider that this satisfies the requirement, unless the entity has actual knowledge of contradictory information. In that case, further verification may be warranted. To ensure clarity and consistency, it would be helpful if the article explicitly stated that obliged entities may rely on customer-provided information unless there are risk factors or

	red flags that would warrant additional verification. In our view, this would support a proportionate, risk-based application. Also, making inquiries on and collecting nationalities may raise concerns about potential discrimination.
5 – Documents for the verification of the identity	We interpret that information as listed in Article 22(1)(a) AMLR serves to identify the customer. For verification of the identity of the customer a limited set of information (i.e., names, surnames and date of birth) suffices. Only in case of reasonable doubts, other identification information could also be verified. We interpret paragraph 1 of Article 5 as applying only to documents that are not official passports or national identity documents and understand that this article establishes an exhaustive list of features that a document must contain in order to be treated as equivalent to a passport or national identity document for the purpose of verifying a customer's identity, in line with Article 22(6)(a) AMLR. Where the document presented is a valid passport or national identity document issued by a state or public authority (e.g., in the Netherlands ID card, driving license), we understand that this can be accepted without further conditions, even if certain elements listed in Article 5(1) are missing. For example, a passport that does not contain an MRZ does not have to be excluded from use if it is a valid government-issued identity document. This should not only be applicable to lower risk situations as mentioned in recital 14. Similarly, with reference to Article 31(3) of the RTS, where e-wallets under eIDAS are used, we assume that any missing attributes may be obtained and where necessary verified through alternative means. Moreover, under eIDAS, specifically Table 1 of Commission Implementing Regulation (EU) 2027/2977, only one of the two data points, place or country of birth, is required. Why is a stricter requirement proposed in the RTS? Is this a deliberate deviation, especially considering that the annex to this RTS refers to this Regulation? We consider that these criteria can be interpreted with sufficient flexibility to accommodate valid identity documents commonly accepted under domestic legislation. For instance, regarding Article 5(2) and Article 3 of the RTS, we note that

not all identification documents provide the country of birth or nationality. We interpret Article 5(2) to allow for reasonable flexibility, whereby such identification documents are still acceptable, and any missing data can be supplemented by information provided by the customer. This applies equally to information such as the usual place of residence, which is not included in most identification documents but is required under Article 22(1)(a) AMLR to identify a customer. Such information will be gathered directly from the customer.

We assume that where the identity of a customer has already been verified under national legislation prior to the AMLR becoming applicable, this verification remains valid and there is no obligation to re-verify a customer's identity merely because the document no longer meets all the conditions of Article 5(1) of the RTS. Once the identity has been verified, it remains valid, unless risk-based triggers indicate a need for renewed verification. Similar as for Article 22(2) of the RTS, we assume that re-verification is not required.

In line with recital 7, we strongly emphasise the need for flexibility in accepting identity documents for customers such as refugees or persons from jurisdictions where standardised identity documentation is not widely available. In such cases, we consider that obliged entities must retain the discretion to determine equivalence on a case-by-case basis, based on its source, reliability and the specific context.

Regarding paragraph 4, we propose clarification that the reference to "a foreign language" should be interpreted as "a language for which the obliged entity does not have the means to understand." Additionally, certified translations should not be mandatory where the obliged entity can reasonably determine the content of the document through other means, such as (online) translation tools or existing internal expertise.

Regarding paragraph 5, the terms "provide" and "certified" require further clarification, particularly in the context of remote or online onboarding. We interpret the term "provide" to mean that the customer must make the identification document available to the obliged entity, either in person or through secure digital means in line with Article 6, including digital uploads in secure portals; and that "certified" be defined in a way that reflects practices in both physical and digital certification. The RTS must clarify who is authorised to perform certifications. We interpret "certified" as confirmation that a copy matches the original, with flexibility for obliged

	entities to determine how and by whom this is done, and to assess the reliability of the certification. We propose clarifying the concept of “any person purporting to act on their behalf” as mentioned in Article 22(6) AMLR. We interpret this as persons acting towards the obliged entity.
6 – Verification of the customer in a non-face-to-face context	**Question 2** *Do you have any comments regarding Article 6 on the verification of the customer in a non-face-to-face context? Do you think that the remote solutions, as described under Article 6 paragraphs 2-6 would provide the same level of protection against identity fraud as the electronic identification means described under Article 6 paragraph 1 (i.e. e-IDAS compliant solutions)? Do you think that the use of such remote solutions should be considered only temporary, until such time when e-IDAS compliant solutions are made available? Please explain your reasoning.* We suggest the EBA considers proportionality and practicality in these cases, allowing a risk-based approach when verifying documents that do not contain advanced security features. While we acknowledge the importance of secure identity verification, the current drafting risks creating rigid, operationally challenging requirements that may undermine customer experience and limit the flexibility of obliged entities to tailor their onboarding process. Specifically, Article 6(1) makes the use of eIDs at a “substantial” or “high” level of assurance or qualified trust services mandatory, if such means are available. This requirement is unnecessarily restrictive and inconsistent with Article 22(6) AMLR, which does not impose a mandatory obligation to use such tools. In practice, eIDs and qualified trust services can introduce frictions into the onboarding process due to redirects or non-responsive systems, potentially resulting in higher drop-out rates. Moreover, the practical functioning of the EU digital identity wallet is still unclear, particularly in cross-border non-face-to-face context, making a meaningful comparison with other remote verification methods premature. Article 6(5) appears inconsistent with the context of non-face-to-face identification. If the original document is not presented physically, features such as holograms cannot be examined as indicators of authenticity. Moreover, obliged entities do not always have the means or expertise to examine such

	features. We recommend clarifying how obliged entities are expected to assess such security features in practice. Regarding holograms, we find that apostilles are more common than holograms and therefore suggest adjusting this paragraph accordingly. Regarding Article 6(3), we request further guidance on what is meant by “this consent must be recorded”, specifically, what form of recording (written, electronic, audio/video) is considered appropriate and sufficient. In addition, the purpose of the consent is ambiguous: consent under EU law must be freely given, implying a real alternative. If no fallback process is provided, the consent becomes de facto mandatory. This may reduce transparency for the customer and lead to meaningless, default consent similar to those seen in cookie policies. It should also be clarified whether such consent may be withdrawn, and if so, what the consequences are for verification and account access. Article 6(6) requires clarification on how obliged entities are expected to demonstrate compliance with the obligation to “examine the security features of the document.” In many cases, especially when onboarding international legal entities, obliged entities rely on copies of foundational documents. These will lack security features and may not lend themselves to authenticity verification without access to external databases or tools not readily available.
7 – Reliable and independent sources of information	We consider that the reference in Article 22(6)(a) AMLR to the use of reliable and independent sources “where relevant” should be interpreted as only relevant where an identity document, passport or equivalent is not available. Further clarification is needed on what constitutes “risk-sensitive measures to assess the credibility of the source.” The current language leaves room for different interpretations, particularly regarding what level of due diligence is expected for different risk categories. We consider that any information obtained from a customer (when there is no contradictory information) can fall within the scope of a reliable and/or independent information in lower risk scenarios, when applied as part of a broader risk-based approach.
9 – Reasonable measures for the	For the verification of the beneficial owner, we propose that reasonable measures may be tailored to the level of risk.

verification of the beneficial owner	Similar as in Article 19. We propose that for non-high risk situations the extract of the central registry suffices for the verification of the identity of the UBO, since the UBO information should already verified by the central registry. For those situations additional confirmation by the customer that their UBO information in the central registry is adequate, accurate and up to date is not proportionate nor risk-based. In all other situations the confirmation of the customer may be requested and where necessary for high risk customers supplemented with additional measures. Remaining question to address, concerns the appropriate measures for legal entities that are not required to register their UBOs in the central registry (e.g. listed companies) In addition, we request clarity in this RTS on who would qualify as an “independent professional”.
10 – Understanding the ownership and control structure of the customer	We consider the requirements under Article 10(1)(b) to be extensive and exceeding what is mandated by Article 62(1)(d) AMLR, particularly as they concern intermediary entities with which there is no business relationship. This would entail a substantial increase of UBO requirements. We recommend aligning the RTS with the AMLR’s scope and providing clarification on how obliged entities can obtain this information efficiently. Regarding Article 10(1)(c), the term “extent of the listing” is unclear. We suggest using “the number or proportion of outstanding shares listed” to reflect transparency obligations under market regulations. Article 10(1)(a), the phrase “…between the customer and their beneficial owners, if any…” seems to imply that in cases where there is no UBO, there is no need to obtain references to intermediary entities. The RTS would benefit from clarification regarding this specific situation.
11 – Understanding the ownership and control structure of the customer in case of complex structures	We find the definition of “complex structure” overly broad. Many international customers generally have multiple ownership layers across jurisdictions. Applying this definition without a risk-based assessment could lead to an unnecessary burden. We recommend allowing for proportionality and risk-based judgment. Additionally, we suggest providing practical examples of “indications of non-transparent ownership with no legitimate economic rationale or justification”.

	The term “organigram” and the information it should contain should be clarified. We interpret “organigram” as the ownership/control path between the customer and the UBO(s), not the entire structure. Where reliable sources are available, obliged entities should not be required to obtain organigrams from customers. The phrase “where there are two or more layers between the customer and the beneficial owner” seems to imply that a complex ownership structure only exists when a UBO is identified. Is it correct to interpret this as meaning that, in cases where there is no UBO, a structure cannot be considered complex? In the phrase: “there are nominee shareholders and/or directors involved in the structure” we interpret “directors” as nominee directors.
12 – Information on senior managing officials	We consider that a business address should suffice for senior managing officials (SMOs). Requiring a residential address is disproportionate and adds limited value. Similarly, nationalities and place of birth of SMOs are not necessary for identification purposes. We believe that name and date of birth, plus business address, are sufficient to identify SMOs. There should not be a verification requirement.
13 & 14 – Identification and verification of beneficiaries of trusts	We suggest clarifying what constitutes “sufficient information” under both articles, e.g. by providing practical examples, especially for complex trust structures or where information is not publicly available. In Article 14(2)(b), we recommend adding the word “reasonable” before “measures” to reinforce that a risk-based approach is permitted, as this aligns with the principle of proportionality and existing AML/CFT practices.

Question 3: Section 1: Information to be collected for identification and verification purposes

Do you have any comments regarding Article 8 on virtual IBANs? If so, please explain your reasoning.

NVB reaction

Article 8 of this RTS as well as Article 2 AMLR lack a clear and unambiguous definition of virtual IBANS, which would encompass various manifestations of virtual

IBANs. This leads to inconsistent interpretation which makes it difficult to currently provide input on this article.

Question 4: Section 2: Purpose and intended nature of the business relationship or the occasional transactions

Do you agree with the proposals as set out in Section 2 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

NVB reaction

As currently drafted, Articles 15 and 16 read more as a template for EDD in high risk situations and not as a proportional and risk-based framework for normal or simplified CDD. We urge the EBA to revise these articles in line with the risk-based approach and allow obliged entities the opportunity to tailor their information collection based on actual risk. Articles 20(1)C and 25 of the AMLR define that information must be obtained as appropriate / where necessary to understand the purpose and intended nature of the business relationship. Expansion beyond this without clear high risk indications would not be proportionate. A proportional risk-based approach tailored to the identified risks should be applied for all risk situations.

We consider Articles 15 and 16 of the RTS to be highly prescriptive and not in line with the risk-based approach. These provisions set out an extensive list of requirements that appear to disregard the necessity for proportionality and risk-sensitivity, particularly in non-high risk situations. We do not see the need for collection of all the information listed in Articles 15 and 16 for normal CDD.

The granular nature of the information to be obtained under these Articles leaves little to no room for obliged entities to apply discretion based on the actual identified level of ML/TF risk. In cases where there are no risk indicators and a customer poses a non-high risk, requiring such extensive data collection is neither proportionate nor effective. Rather, it creates unnecessary friction in business relationships with well-intended customers, negatively impacting customer experience and diverting resources from higher risk cases. It might also warrant unnecessary customer outreach even when the purpose and intended nature can already be inferred from the product and existing or intended relationship.

For example, the requirement to obtain detailed information on a customer's employment income (including salary, wages, bonuses, pension or retirement funds, government benefits, business revenue, savings, loans, investment income, inheritance, gifts, and other asset disposals) is excessive in the absence of any risk indicators. In a normal CDD context, this information does not contribute meaningfully to the risk assessment or the understanding of the business relationship. Such data collection should only be triggered where the nature of the relationship or transaction raises specific concerns that warrant further investigation.

Similarly, the expectation to collect information about the expected type(s) of recipients, jurisdictions of incoming transactions, and comprehensive details about the

customer's occupation (including the sector, industry, operations, products and services, regulatory status, geographic footprint, and revenue streams of the employer) is disproportionate for a natural person opening a payment account or engaging in routine transactions.

Article 15(d), which stipulates that obliged entities must determine the source of wealth where the ML/TF risk is higher, also raises concern. Even within the context of EDD, determining the source of wealth should not be a standard requirement (see our comments to Article 27). It is an intrusive measure that should be applied selectively and only in clearly high-risk scenarios. Treating it as a standard obligation in any higher risk context is counterproductive and inconsistent with effective risk prioritisation.

Question 5: Section 3: Politically Exposed Persons
Do you agree with the proposals as set out in Section 3 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

NVB reaction
In Article 17 of the Draft RTS on Politically Exposed Persons (PEPs), it should be clarified whether the same level of information requirements applies to relatives and close associates (RCAs) of PEPs as to the PEPs themselves. We consider that for RCAs, an even more risk-based approach should apply, based on the nature of the relationship and the risk profile of the individual.

We propose to explicitly state that the use of automated screening tools can fulfil the compliance obligation to determine whether an existing customer, the beneficial owner, or - where relevant - the person on whose behalf or for whose benefit a transaction or activity is carried out, has become a PEP. The RTS should confirm that obliged entities are not required to obtain from each identified PEP a complete list of all family members and close associates. Such an obligation would be disproportionate and intrusive.

For low-risk PEPs, including those whose PEP status results from a function held in the past or from a low-risk role, information collection should follow a proportionate, risk-based approach. Obliged entities should not be expected to make inquiries directly with the customer in the absence of risk indicators.

It should be explicitly recognised that it is more necessary to collect PEP-related information from newly onboarded PEP-customers than from existing customers becoming a PEP with whom there is a well-established longstanding relationship. In those latter cases, obliged entities should be allowed to place reliance on existing knowledge and historical customer data, without the immediate need for customer outreach.

Question 6: Section 4: Simplified Due Diligence measures
Do you agree with the proposals as set out in Section 4 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

NVB reaction
We would like clarification on the difference between “lower risk situations” as referenced in Article 18 and “low risk situations” as referenced in the title of Article 19, and how both relate to the terminology used in Article 33 AMLR, which refers to a “low degree of risk”. It is important that terminology across regulatory instruments is aligned or clearly distinguished.

In practice, different obliged entities use varying definitions and categories for customer risk levels. It would be helpful if the final RTS acknowledges this variation. We assume that the term “low(er) risk” in these articles implies any situation that is not considered “high risk”. Confirmation of this interpretation would be useful to ensure consistent application across the industry. Also considering that the vast majority of customers is non-high risk. The recently published report on integrity supervision by DNB provided relevant insights into the number high-risk customers in the Netherlands. From 2022 to 2023 there is a decreasing trend which amounts in 2023 to ~142k private individuals classified as high risk and ~100k business clients. These figures should be interpreted in the context of ~35.9 million banking relationships in the Netherlands.

Regarding Article 19, we understand this to mean that where the obliged entity holds official data from a reliable register such as a chamber of commerce or central UBO-registry, confirmation by the customer of the extract is sufficient and would not be necessary for non-high risk customers – as already verified by the central registry. We support this interpretation and seek confirmation of this understanding. Currently we experience significant differences in quality and use of central registers within the EU. To attain a level playing field, we advocate further harmonisation between central registers.

On Article 22, we interpret this to mean that in non-high risk situations - i.e., where there are no indicators of high risk - the obliged entity may rely on its risk and event triggers (e.g., transaction monitoring systems). Where no risk triggers have been identified, there should be no need to actively request identification information from the customer, meaning that data correctness does not expire until there are reasons to doubt the correctness of customer data and information. Paragraph 2 of this article would need to support this reading, in that if the monitoring process is effective, it would have flagged any relevant events, eliminating the need for additional outreach to customers. Moreover, when no material changes in customer information or behaviour are demonstrated, the customer file can be considered automated reviewed.

Specifically, under Article 22 c): what would be considered “unexpected transactions”?

On Article 23, we consider that the reference to understanding the source of funds in this article is not aligned with Article 20(1)(f) AMLR, which treats source of funds as part of ongoing monitoring and only “where necessary”.

In general, we notice that the articles in Section 4 are stricter than the AMLR, i.e. for source of funds and purpose and intended nature. In low(er) risk situations, the purpose and intended nature of the business relationship should primarily be derived from the type of product or service the customer obtains from the obliged entity. There is also no basis to require source of funds information by default. Doing so would undermine the principle of proportionality and the concept of SDD.

Question 7: Section 4: Simplified Due Diligence measures
What are the specific sectors or financial products or services which, because they are associated with lower ML/TF risks, should benefit from specific sectoral simplified due diligence measures to be explicitly spelled out under Section 4 of the daft RTS? Please explain your rationale and provide evidence.

NVB reaction
Recital 127 AMLR states that for listed companies and bodies governed by public law of the Member States beneficial ownership and control is of a similar level of transparency and there is no need to apply beneficial ownership requirements. We therefore propose to exempt the obligation for obliged entities to identify UBOs in these situations. If not feasible, we suggest limiting the obligation to register SMOs for these types of legal entities.

Recital 113 AMLR states that due to the specific nature of certain legal entities, it is not meaningful to identify beneficial owners based on ownership or membership. In those cases, we propose to exempt these entities from the obligation to register UBOs in the central register and exempt obliged entities from the obligation to identify UBOs in these cases.

SWIFT RMA relationships are by banks not viewed as constituting a business relationship and thus pose no direct ML/TF risks (more detail is included in the paragraphs below). Likewise, where a customer is government-funded in a non-high risk country, the risk is inherently lower due to public oversight and transparency. We recommend these cases to be explicitly included under Section 4 as eligible for SDD measures.

Regarding the SWIFT RMA relationships we suggest removing as a risk reducing factor, as per the 2021 EBA CDD and Risk Factor Guidelines. Its inclusion implies that these relationships qualify as (correspondent) relationships. The exclusion of SWIFT RMA-relationships is also seen in recital 43 of AMLD5, reading as a paraphrasing of the FATF and supported by a.o., the Wolfsberg Group. Both market practice and operational reality support excluding SWIFT RMA-relationships from the concept of correspondent banking relationships.

The ability of financial institutions to exchange messages across the SWIFT network (reachability) is central to the functioning of the global banking system. Doing so, in absence of the provision of any products or services to the RMA connected financial institution (e.g., payment initiation capabilities), does not constitute a (correspondent) relationship. This further implies that no customer relationship is considered to exist, and CDD is applicable. We support the application of proportionate and risk-based risk management measures for such relationships. However, the underlying risk is an operational risk, not an AML/CTF risk.

Question 8: Section 5: Enhanced Due Diligence measures
Do you agree with the proposals as set out in Section 5 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

NVB reaction
We are concerned that several EDD provisions impose overly rigid requirements. As noted in our earlier comments, we recommend incorporating clearer references to the risk-based approach, allowing obliged entities to tailor EDD measures to the actual risk exposure. EDD is only meaningful when it is targeted to mitigate specific risks. In some cases, existing information already held by obliged entities may suffice to meet EDD requirements. This observation applies to all EDD-related articles discussed below.

The below table lists our reaction and suggestions regarding the articles in Section 5.

Article	Consultation reaction
24 - Additional information on the customer and the beneficial owners	We note that the wording “at least” in Article 24 introduces what appears to be a mandatory minimum list of additional information to be obtained by obliged entities. This appears to conflict with Article 34(4) AMLR, which states that EDD measures shall be proportionate to the higher risks identified. The phrasing in Article 24, specifically “shall, at least” and the use of “and/or”, is ambiguous. It is unclear whether obliged entities are required to obtain all the information listed under subparagraphs (a) to (d), or any one of them. To resolve this conflict and improve clarity, we recommend replacing “at least” with “where necessary”, thereby aligning the article with the proportionality principle in Article 34 AMLR. On a) we interpret the reference to “or the ownership and control structure” as applying only when relevant, and we seek clarification on what constitutes “verification of authenticity”. What are the minimum expectations regarding sources or documentation?

	On b) we welcome the explicit recognition of adverse media screening as an EDD-measure. This affirms our current approach and supports proportional application. On c) we interpret the reference to past business activities to be applicable only when risk relevant, and request clarification on the expected time horizon for such assessments, to avoid unnecessary data collection. On d) we emphasise that, while a holistic understanding of the customer is important, requesting information on family members, close associates, or business partners may: i) be conflicting with GDPR requirements; ii) in some cases, risk tipping-off, particularly in SAR context. Furthermore, this may cross into areas that fall under law enforcement rather than AML compliance, especially when the obliged entity has no business relationship with those family members or close associates. Any such requirements should be proportionate, supported by an immediate cause for assuming a relevant link to criminal activity.
25 – Additional information on the intended nature of the business relationship	Regarding a), the requirement for obliged entities to verify the legitimacy of the destination of funds raises questions about feasibility and scope. Specifically, it is unclear what “information from authorities” entails. Does this imply that obliged entities are expected to contact domestic or foreign tax authorities or FIUs to verify where the funds are going? Such an expectation would be disproportionate, operationally impractical, and potentially conflict with the GDPR and the risk-based approach. On b), we would like clarification of what is expected when obliged entities are asked to verify the legitimacy of the expected number, size, volume, and frequency of transactions. If this implies substantiating each transaction with invoices, agreements, tax statements, or receipts for daily expenses such as food or utilities, it would be an extremely burdensome and unrealistic requirement for both customers and obliged entities. We consider that this, if required, such verification must be aimed at risk mitigation rather than obtaining documentation for technical compliance. In relation to c), we question how the requirements in Article 25 align with the already extensive obligations under Articles 15 and 16 concerning the purpose and intended nature of the business relationship as there appears to be overlap. Additionally, we seek assurance that this article does not

	imply a requirement to perform CDD on the customer's clients or counterparties, as this would expand the scope of due diligence obligations beyond what is intended under the AML/CFT framework.
26 – Additional information on the source of funds, and source of wealth of the customer and of the beneficial owners	The requirement to verify that the source of funds or source of wealth is derived from lawful activities using one or more forms of evidence sets an extremely high bar even as an EDD measure. This appears to reflect expectations more appropriate for forensic auditors or law enforcement investigations rather than for obliged entities conducting CDD in accordance with a risk-based approach. Regarding a), the expectation that pay slips or employment documentation must be signed by the employer is outdated and incompatible with modern digital payroll systems, where physical signatures are not the norm. In relation to b), requiring certified copies of audited accounts raises the question of who is expected to provide the certification. If the accounts are already audited by an audit firm, their signature should suffice—additional certification should not be necessary. Similarly, for all requirements for "certified copies", the RTS must clarify who is authorised to perform such certification. If an obliged entity has seen the original document, it should be permissible for the entity to retain a copy and certify that it has reviewed the original, without requiring external certification. Regarding d), for assets stemming from inheritance, the availability of public official documentation cannot be assumed. In many jurisdictions, inheritance may be settled informally within families where the legal heir is obvious and no will exists. Such cases should be accommodated with alternative forms of evidence or declarations.
27 – Additional information on the reasons for the intended or performed transactions and their consistency with the business relationship	In relation to b), we request further clarification on how "consistency" is to be determined and what criteria are to be used to evaluate whether transactions align with the customer's business activities and turnover. Should we understand "assets representing higher risks" to refer to business activities where there are large price fluctuations, high-value low-volume assets, or high-value transactions?

	With reference to c), the obligation to assess the legitimacy of the parties involved in a transaction, including intermediaries and their relationship to the customer, appears to imply a requirement to conduct CDD on the customer's business partners. This is neither feasible nor appropriate for obliged entities and should not be part of the EDD requirements. Furthermore, where the counterparty is a customer of another bank, specifically when located in the EU, obliged entities should be permitted to rely on the presumption that the counterparty's bank has fulfilled its CDD obligations according to EU laws and regulations. We propose that even in high-risk situations requiring EDD, if a transaction is within the expected transaction profile of the customer and consistent with the purpose and nature of the business relationship, it should not trigger an obligation to conduct additional scrutiny. EDD should focus on deviations from expected behaviour. Paragraph d) seems to imply that obliged entities should gather information on non-customers in case of reasonable grounds to suspect criminal activity. There is no legal basis to collect information on non-customers, and the intention of this article is not clear and may lead to privacy issues.

Question 9: Section 6: Targeted Financial Sanctions
Do you agree with the proposals as set out in Section 6 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

NVB reaction
Regarding Article 28, we consider that the reference to "all the entities or persons which own or control such customers" must be interpreted in line with Article 20(1)(d) AMLR. We therefore seek confirmation that this provision refers specifically to the person or entities that control the customer or have more than 50% of the proprietary rights of the customer. Similar for Article 29(a) sub iv.

Similarly, as the SMO is not a UBO, we consider that there is no need to screen the SMO, particularly since the customer's assets are not linked to the SMO's assets and would not be subject to freezing in the event of a positive sanctions hit.

We note that several provisions in Article 29 diverge from the established expectations in EBA/GL/2024/15 on sanctions screening, without clear justification.

- a) sub i. requires screening of "all first names and surnames", whereas EBA/GL/2024/15 (paragraph 17) refers to "the first name and surname". Why this broader scope?

- a) sub iii. includes no option to deviate from the obligation, unlike the flexibility allowed in paragraph 17 of the Guidelines. How do these differences align? This provision assumes full availability of all listed datapoints for sanctions screening. Whereas data such as wallet addresses and aliases are not obligatory. Therefore, we propose to change the wording to “where available for obliged entities”.
- a) sub iv. mandates screening against beneficial ownership data, but without defining which data. Paragraph 18 of the Guidelines distinguishes between ownership, control, and acting on behalf. Why was this more nuanced approach not adopted? Additionally, we seek confirmation that the reference to beneficial ownership information means persons that control the customer or have more than 50% of the proprietary rights of the customer.
- c) sub iii would benefit from clarification if a “change of residence”, being someone moving to a new address (even in the same city or country where someone lives), indeed is a situation that necessitates screening.
- d) uses “without undue delay”, while the Guidelines and the Instant Payments Regulation require screening “immediately”. Clarification on the intended standard would be welcome.

Question 10: Section 7: Risk factors associated with features of electronic money instruments

Do you agree with the proposals as set out in Section 7 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

NVB reaction

With the requirements set forth in Article 30 we note that applying the exemption for electronic money instrument will be practically impossible

Question 11: Section 8: Electronic identification means and relevant qualified trust services

Do you agree with the proposals as set out in Section 8 of the draft RTS (and in Annex I linked to it)? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

NVB reaction

For our reaction on this question, we refer to our input provided for question 1. We are surprised no mention is made on active user verification in Article 31. We suggest introducing this as an obligation in this article.

NVB reaction to Article 32 – Grace period for updating customer information

We interpret Article 32 of the RTS on CDD to introduce a five-year period within which all customer identification data must be updated for existing customers, in accordance with Article 22(1) of this RTS. In our view, customer identification data includes all CDD elements, such as the identification of the customer (name and date of birth),

ownership and control structure, UBO, SMO, and legal representatives. This reading is consistent with recital 16 of the RTS and recital 43 of the broader EBA consultation document. Furthermore, we would like to point out a -most likely - erroneous reference to Article 23(1) of this regulation in Article 32 on the entry into force.

Although Article 32 refers to the entry into force of this Regulation (being this RTS on CDD), we consider that the five-year period is intended to begin from the application date of Regulation (EU) 2024/1624 (the AMLR), as confirmed in Article 90 AMLR, which sets this date as 10 July 2027. Recital 16 of the RTS supports this interpretation by explicitly referring to the “application date” as the moment from which the update obligation should be calculated. Accordingly, we interpret Article 32 to mean that all existing customer information must be updated, in a risk-based manner, by no later than 10 July 2032.

In line with recital 43, we will prioritise customer files that present a higher risk. The order in which banks will review and update lower risk customers will be based on the banks’ internal risk assessments and ensuring compliance within the five-year timeframe.

In addition, banks will treat event-driven reviews - such as alerts, unusual transactions, or other relevant risk indicators - as a trigger to update the customer identification information, irrespective of the originally planned periodic review cycle.

Finally, while the obligation to update information formally applies from 10 July 2027, we are of the opinion that obliged entities may begin updating identification data before that date where operationally feasible. Also considering that it may result in avoiding repeated customer outreach in a relatively short period of time. Given that the AMLR has already entered into force, we have concluded that early updates are supported by a legitimate interest under the GDPR and will enable operational readiness.

B) Draft RTS on the assessment of the inherent and residual risk profile of obliged entities under Article 40(2) of the AMLD; and 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 under Article 12(7) of the AMLAR

NVB reaction

These proposed RTSs represent an important step in ensuring consistency in how inherent and residual risk profiles of obliged entities are assessed across Member States. However, we would like to express several concerns regarding the practical implementation of these frameworks, in particular relating to the collection and use of data, and the timeline foreseen. We urge the EBA to ensure that the implementation of these RTSs allows for a phased and practical approach.

In recent years, supervisors have already been collecting AML/CFT-related data points from obliged entities. This has provided useful lessons, particularly around the need for clarity and precision on definitions, and alignment in data requirements. The data points to be proposed under these RTSs may differ significantly from what has previously been collected, and in many cases, new or adjusted internal systems might be necessary to comply with the requirements. In this light, we believe a transitional approach is warranted.

We recommend that a transitional period be explicitly included like the one proposed in the RTS on the selection for direct supervision (recital 7). For the first two years following entry into force, the reporting of data should be treated as a best-effort obligation, allowing obliged entities time to embed new requirements into their systems. Moreover, after the first year, a review of the data points should take place, assessing their usefulness, necessity, burden imposed and clarity of the definitions. The overall process should be recognised as iterative, with room for refinement and improvement based on actual application and dialogue between supervisors and obliged entities.

In addition, we would like to highlight the importance of clear definitions for the data to be collected. Experience has shown that ambiguities around concepts such as the definition of types of customers or transactions can lead to divergent interpretations, which in turn undermine the comparability and reliability of risk assessments. We expect that the accompanying interpretive note with hold extensive clarification on the datapoints and allow sufficient time for obliged entities to adjust their processes, systems and reporting.

For reporting by a group, it is essential to clarify how obliged entities should treat customers that are customers of multiple group entities, how intragroup transactions are to be treated, and whether consolidation should apply to all group entities globally, or only to those within the EU, or only those that are obliged entities.

We also emphasise the need for adequate time to collect and report the data. Given the number and granularity of the required data points, there will likely be a notable increase in compliance costs. Establishing the necessary systems and data quality checks will take time, and reporting timelines should reflect this reality. The requirement to assess and classify the risk profile of obliged entities at least annually, by 30 September, should be determined if realistic.

C) Draft RTS under Article 53(10) of AMLD6 on pecuniary sanctions and administrative measures

NVB reaction

We note that the effectiveness of this RTS may be limited by the current divergence in the legal qualification and enforcement of AML/CFT breaches across jurisdictions.

We are concerned that differences between criminal and administrative enforcement could undermine the intended harmonisation. In some Member States, such as the Netherlands, AML/CFT breaches, even if committed negligently or unintentionally, can constitute an economic crime, leading to direct criminal prosecution. In contrast, other Member States may treat even intentional breaches administratively. This divergence may lead to unequal treatment of obliged entities, depending on their jurisdiction, and creates an unlevel playing field.

This discrepancy is especially problematic when considering the role of cooperation during supervisory examinations. The *nemo tenetur* principle applies when breaches may have criminal consequences, meaning that obliged entities may refrain from sharing information to protect their legal position. However, under Article 4(3) of the draft RTS, a lack of cooperation may result in higher fines, placing entities in a difficult and conflicting position, either cooperate and risk prosecution, or remain silent and risk an aggravated sanction. This outcome seems at odds with the fairness and proportionality principles underlying this RTS.

Moreover, the RTS emphasises the need for supervisors to ensure consistent and comparable outcomes across Member States, including a common understanding of the gravity of breaches. This consistency will be hard to achieve as long as non-intentional breaches trigger criminal law in some Member States but not in others. A genuinely harmonised and risk-based approach to sanctions requires that the underlying legal frameworks across Member States be aligned, particularly in how they distinguish between administrative and criminal responses.