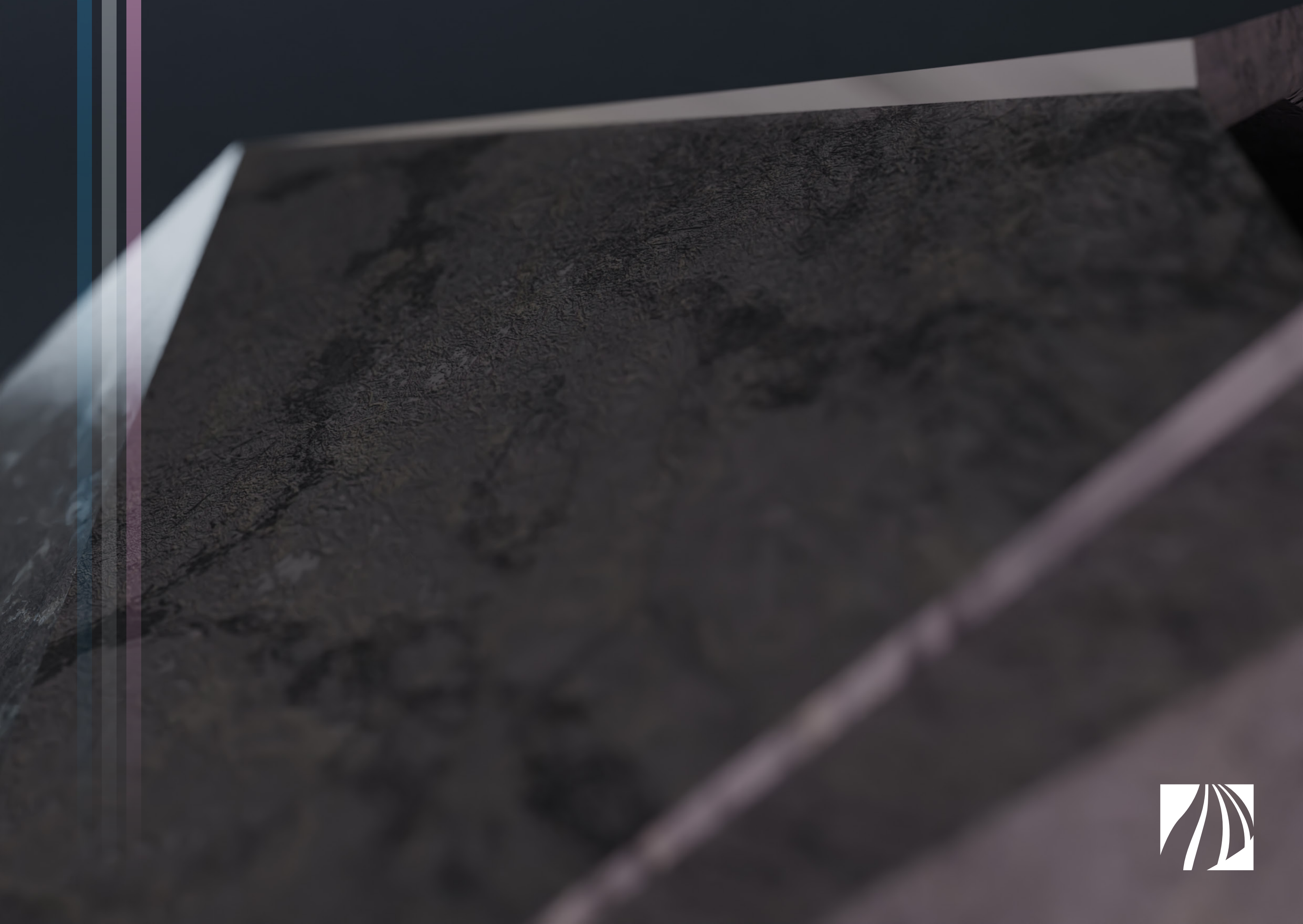
NOVEMBER 2023

REGCOUNSEL FINANCIAL SERVICES WHITE PAPER SERIES #1

The NVB Industry Baselines and DNB Good Practices
on the risk-based implementation of the AML Act



ABOUT THE AUTHORS

Mr. dr. drs. Jan A. Jans is a specialist in financial regulatory law. He has a strong focus on the regulatory framework covering banks, insurance companies, payment service providers, investment firms and investment funds. Prior to joining Regulatory Counsel I Financial Services as partner in 2022, Jan Jans worked as a financial regulatory lawyer at various (international) law firms in the Netherlands.

Jan Jans graduated from Nijmegen University in 2008. In addition to law, he studied financial economics and business administration. He completed the post-academic education Securities Law at the Grotius Academy in 2012. Jan publishes regularly in national law journals and successfully defended his PhD thesis on the level playing field between banks and non-banks in the European market for electronic payments in February 2023.

✉ Jan.jans@recofise.eu ☎ +31 6 83 50 49 27

Maarten Mol-Huging LLM graduated cum laude at the VU Amsterdam in International Business Law in 2022 on his thesis titled: The Biggest Challenge yet for EU Mortgage Lending: The Onset of Artificial Intelligence Tooling. He advises on financial regulatory issues with regards to banks, investment firms, insurers, payment service providers and FinTech (e.g. digital asset service providers).

Before the VU, Maarten obtained a Dutch law Bachelors at the Rijksuniversiteit Groningen, where he was on the board of the corporate law study association. To further build his knowledge of EU financial regulation he is pursuing the EBI master in EU Banking and Financial Regulation at the Frankfurt School of Finance and Management since fall 2022.

✉ Maarten.mol-huging@recofise.eu ☎ +31 6 29 90 96 29

Recofise is a boutique law firm located in Amsterdam which specialises in financial regulation. Our clientele consists of financial institutions (e.g. banks, investment firms, insurance companies, electronic money institutions and payment institutions) that are active on the Dutch and international financial markets. We have over 30 years of experience in advising and supporting clients with complex legal issues regarding compliance, risk management, supervisory reporting and supervisory audits.

TABLE OF CONTENTS

1. THE INDUSTRY BASELINES AND DNB Q&A AND GOOD PRACTICES

1. THE INDUSTRY BASELINES AND DNB Q&A AND GOOD PRACTICES

In 2023, the Dutch Banking Association (*Nederlandse Vereniging van Banken* '**NVB**') has published new risk-based industry baselines (the '**Industry Baselines**') wherein principles are contained that banks can apply in their risk-based implementation of the open norms of the Dutch AML Act (*Wet ter voorkoming van witwassen en financieren van terrorisme* '**AML Act**'). These Industry Baselines have been coordinated with the Dutch Central Bank (*De Nederlandsche Bank* '**DNB**') and the Dutch Minister of Finance, being the responsible bodies for the supervision on the correct application of the AML Act requirements by certain 'obliged entities', including banks, which gives a certain level of authority to the Industry Baselines.

In this paper, RegCounsel Financial Services highlights the main elements of the Industry Baselines that have been issued recently as well as their implications for obliged entities in the context of the current legislative framework. At the end of the overview we conclude that, although the issued and future Industry Baselines will provide for an important source of guidance for the risk-based approach of the AML Act obligations, the proper foundation in law of some of these Industry Baselines can be questioned.[1] This latter point becomes especially relevant and urgent when tested against the forthcoming Anti-Money Laundering Regulation ('**AMLR**')[2] which contains several provisions that seem to be at odds with certain positions taken in the Industry Baselines. Nevertheless, it seems that a lot of the conclusions of the Industry Baselines are shared by DNB, with the occasional technical deviation.

The first Industry Baselines were published on 30 May 2023 and see to the following subjects: (a) Enhanced Due Diligence Measures for European Commission High Risk Third Countries ('**EDD EC HRTC**'); (b) UBO identification and verification; (c) Pseudo-UBO; (d) Expected Transaction Profile ('**ETP**'); (e) Data actualisation (part of Ongoing Due Diligence).[3] Below, we discuss each of these Industry Baselines in reference to the corresponding legislative framework as contained in the AML Act, the fourth Anti-Money Laundering Directive ('**AMLD4**') and relevant guidance documents published by supervisors, regulators and private initiatives, such as the DNB Guidance on the application of the AML Act and the Sanctions Act ('**DNB**

[1] A key indication for this doubt can be found in a recent judgement where the court considered that a more lenient interpretation of the risk-based approach included in the current regulatory framework forwarded by DNB in the report From Recovery to Balance (see n50) (freely translated): 'Moreover, it is important to note that the [DNB Report] only contains proposals to amend legislation and is therefore about possible (uncertain) future amendments of legislation.' District Court Rotterdam, 31 August 2023, Claimant/DNB, ECLI:NL:RBROT:2023:8237, r.o. 28.

[2] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, (2021).

[3] NVB Press Release, Minder klantimpact door NVB Standaarden voor risico gebaseerd witwasonderzoek, 30 May 2023.

Guidance').[4] We note that the Industry Baselines are not legally binding and have been developed as a set of guiding principles for banks. However, the NVB itself notes that the Industry Baselines may be used by other parties as well, albeit mostly for understanding the modus operandi of banks. The DNB consultation on Q&A and Good Practices under the AML Act, which was published on 18 October 2023 ('**DNB Q&A and Good Practices**'), explicitly refers to the Industry Baselines and expands the scope of its own report to all obliged entities. Therefore, we refer to banks in this paper when discussing the Industry Baselines and to obliged entities pursuant to art. 1a AML Act when discussing points of general application for other (financial sector) obliged entities (such as payment institutions).[5] However, it may be to a large extent assumed that the conclusions of the Industry Baselines can be extrapolated to all other obliged entities.

A second set of Industry Baselines was published on 17 July 2023 addressing (f) the Ongoing Due Diligence requirements and (g) the models used in alert and event generation. These Industry Baselines are a much-needed addition of the first set of Industry Baselines as these raise questions as to the underlying assumptions of some of the risk-based processes described therein. Most recently, the NVB published the (h) Not-for-Profit Organisations ('**NPO**') Industry Baseline, further clarifying the AML Act application to this specific sector. The latest Industry Baseline was published by the NVB in November 2023 and covers so-called crypto-asset service providers ('**CASPs**').

The DNB Q&A and Good Practices provide for the long anticipated review of the existing DNB Guidance, excluding the part with respect to the Sanctions Act (*Sanctiewet 1977* '**Sanctions Act**'), in line with the announcements made for a more balanced AML approach by DNB in its December 2022 report entitled 'From Recovery to Balance'.[6]

The DNB Q&A and Good Practices must be understood as the formalisation of a more amenable interpretation by DNB of the AML Act, whilst simultaneously meeting the market's outcry for more practical tools to form their AML policies and procedures. A newly interpreted risk-based approach to AML takes the centre stage in this reworked framework, perhaps best expressed by DNB itself: 'As part of risk management, the institution applies mitigating measures to the business

[4] DNB, Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act: December 2020 Version, (2022).

[5] In the case referenced in n1 above, the court considered that the DNB Report (n50), which can be seen as the fundament under the NVB Industry Baselines, cannot mechanically be relied upon nor its conclusions extrapolated to other obliged entities.

[6] DNB, From recovery to balance A look ahead to a more risk-based approach to preventing and combating money laundering and terrorist financing, (2022).

relationship. The level of control should match the client’s risk profile: the intensity of the measures to prevent money laundering and terrorist financing should be tailored to the concrete risks posed by a client. An increased risk requires more attention, while a lower risk requires less intensive control.’[7]

It must preliminary be concluded that the DNB Q&A and Good Practices have achieved a level of clarity that has been lacking until now. There are several points where concrete risk-based guidance is given, without restricting diverging approaches if those appear more suitable to the obliged entity and it can substantiate them as such. Nevertheless, there are some points where DNB remains ambiguous and does not provide concrete guidance. Moreover, there are some passages in the DNB Q&A and Good Practices of which the legality could be questioned given that they do not always seem to align with the AML Act and AMLD4.

It must be understood that the new guidance documents, both of the NVB and DNB, have not been produced against a new legal background, the AML Act and the AMLD4 remain unaltered as compared to the regime against which the old DNB Guidelines were produced.

[7] DNB Q&A and Good Practices, paragraph 3.11.

2.EDD EC HRTC INDUSTRY BASELINE

2. EDD EC HRTC INDUSTRY BASELINE

This Industry Baseline addresses Enhanced Due Diligence (‘**EDD**’) measures that need to be applied, pursuant to art. 9 AML Act,[8] when a business relationship or a transaction is performed involving a jurisdiction that has been designated as a high-risk third-country (‘**HRTC**’) by the Commission in accordance with art. 9(2) AMLD4. Principally, the Industry Baseline concludes that a bank must assess whether the transaction involving a HRTC presents a low, medium or high risk by assessing: (i) whether the transaction was to be expected given the transaction profile and behaviour of the business relationship involved; and (ii) the nature of the transaction itself, for example a holiday expense could be made in an HRTC which transaction does not have to be considered high-risk per se.[9] Nonetheless, certain EDD measures must be applied by default in a risk based manner by an obliged entity in case of a transaction involving a HRTC on the basis of the Dutch and EU legislative framework. If a client of an obliged entity, or its UBO is located or domiciled in an HRTC, such client will de facto be high-risk and thus subjected to the additional measures of art. 8 AML Act.[10]

In the circumstances where a bank is presented with a low or medium risk HRTC transaction, a bank shall generally be able to sufficiently perform EDD measures with the existing data it has, or it can collect with desk research, thus not necessarily having to turn to the business relationship, i.e. customer, itself for the collection of such additional information, permitting the performance of the EDD.[11] However, if the information that is available can no longer be considered up-to-date or the client involved acted in a manner inconsistent with its risk profile, the obliged entity will have to turn to the client for more data. Furthermore, the decision making on HRTC business relationships will be allowed to take place at a more operational, albeit still senior one echelon lower level than the management board of the obliged entity. This notwithstanding the ultimate responsibility of the management board for the proper observance of the bank’s compliance with the AML Act and the requirement to draft an objective policy setting out the parameters for such decision making.[12] HRTC transactions shall in principle not be subjected to higher management approval and shall instead be covered by the regular ongoing

[8] As also included in art. 18a(2) AMLD4.

[9] DNB Q&A and Good Practices, GP 3.39. Rather, the obliged entity will have to take account of the relevant high-risk indicators, such as those included in the non-limitative list in Annex III of the AMLD4, and must make its own assessment as to whether the client presents a high-risk in the concrete case. Factors that may be considered are method of payment (i.e. cash), location of transaction, type of product or service acquired, sector of business or other risk factors, such as those set out in thew EBA Guidelines in ML/TF Risk Factors.

[10] DNB Q&A and Good Practices, GP 3.41.

[11] DNB Q&A and Good Practices, Q 3.39.

[12] DNB Q&A and Good Practices, GP 3.37.

monitoring of the relationship, provided that they are sufficiently recorded and accounted for in the transaction profile.[13]

A significant change that is suggested in the Industry Baseline is the possibility to forego the application of EDD measures in transaction monitoring where the business relationship was/is subjected to EDD measures at onboarding and review and the transactions involving the HRTC fit the transaction profile and behaviour.[14] In such cases, the NVB concludes that enhanced monitoring of transactions is sufficiently accounted for and EDD measures are not necessary. This exception seems directly conflicting with both art. 9 AML Act and art. 18a AMLD4 and the interpretation thereof by DNB. The Dutch legislature noted in the parliamentary proceedings surrounding the implementation of art. 18a AMLD4 that '[...] the directive [AMLD4] requires these stricter measures. The directive does not allow for derogations from this.'[15] Thus, the exception not to apply EDD measures in transaction monitoring must more be read as a risk-based implementation of EDD measures, that are included in the transaction profile and expected behaviour pattern, including in the scrutiny that the business relationship has been subjected to in the onboarding stage. Later, during the review cycle of the business relationships, (further) EDD measures, as included in art 9(1)(a) to (e) AML Act, are to be applied in addition to the EDD measure of enhanced monitoring, as included in art. 9(1)(f) AML Act, which is observed during the transaction monitoring. This risk-based approach of the requisite EDD measures is also forwarded by DNB, which considers that the intensity of the application of the measures in art. 9 AML Act may vary in proportion to the concrete risk of the given case.[16]

It is imperative that the 'liberalisation' of the DNB Q&A and Good Practices and the EDD HRTC Industry Baseline are in any event supported by proper documentation on each and every instance where the more lenient process is applied, in order to ensure that post res the measures taken can be construed as a proper risk-based approach to the obligation to perform EDD measures in relation to HRTC transactions and business relationships. This requirement of strong documentary evidence holds for all Industry Baselines discussed below as the risk-based approach requires proper explicit reasoning. Therefore, when obliged entities will use the Industry Baselines to adjust their AML/CTF processes this cannot simply be done with a reference to the Industry Baselines, a tailored explanation as to why the change in procedures befits the obliged entity will need to be recorded and should be revised periodically on its merits.

[13] DNB Q&A and Good Practices, GP 3.36 and 3.38.

[14] NVB, Risk Based Industry Baseline: EDD measures for EC high risk third countries, (2023), p.4. See for a similar line of thought paragraph 7, specifically the risk-differentiated reviews.

[15] TK 2018-2019, Kamerstukken 35 245 Nr. 3, p. 30.

[16] DNB Q&A and Good Practices, Q 3.37.

3.

UBO IDENTIFICATION AND VERIFICATION INDUSTRY BASELINE

3. UBO IDENTIFICATION AND VERIFICATION INDUSTRY BASELINE

This Industry Baseline addresses the obligation to identify Ultimate Beneficial Owners (‘**UBOs**’) as part of the CDD process pursuant to art. 3(2)(b) AML Act and to take reasonable measures to verify such identity, the result of which shall have to be recorded accordingly.[17] The CDD requirements surrounding UBOs have been subject of much debate recently due to the Sovim judgement of the European Court of Justice, which closed down the publicly available UBO-registers due to data privacy concerns.[18] As a result, obliged entities had to resort to convoluted intermediate solutions where the customer is asked to issue a UBO-declaration or comparable processes to compensate for the temporary ban (also for obliged entities) for consulting the UBO-Register. These declarations are used to (temporarily) substitute for the unavailability of the UBO-register excerpts which are set to open again shortly in a more restricted form.[19] This issue is reflected in the Industry Baseline, and upheld by DNB, which builds on the temporary practice to enhance the role of the customer in confirming the data, although pivotally not the quantity of information that needs to be requested.

Banks are advised to delineate between low, medium and high-risk customers before identifying and verifying their respective UBOs. Prior to the closure of the UBO-Register low and medium risk Dutch customers’ UBOs could be identified by (i) extracting and recording an excerpt from the UBO-register and (ii) requesting the customer to confirm the information contained therein.[20] A view corroborated by the DNB Guidance and the DNB Q&A and Good Practices.[21] Interestingly, the Industry Baseline makes a distinction for the identification of high-risk Dutch customers, yet the measures regarding identification remain identical, this seems somewhat at odds with the risk-based approach of the AMLD4 and the interpretation thereof by the EBA.[22] The risk-based approach to identification seems to have been reduced to a highly practical, but legally fragile, sole reliance on the UBO-register and a confirmation of the customer without requiring a second

[17] Art. 33(2)(b) AML Act.

[18] ECJ, 22 November 2022, C-37/20 and C-601/20, WM and Sovim/Luxembourg Business Registers, ECLI:EU:C:2022:912.

[19] Recently the Dutch Government opened the public consultation on the law that will reopen the UBO-register for obliged entities. The consultation will close on 28 June 2023 and will most likely be swiftly followed up in order to return to a proper functioning of the UBO framework. Internetconsultaties, Wijzigingswet beperking toegang UBO-registers, (link), (last accessed: 6 June 2023).

[20] NVB, Risk-Based Industry Baseline: UBO identification and verification of the UBO’s identity, (2023), p. 4.

[21] DNB, Leidraad Wwft en SW: Versie December 2020, (2022), p. 37 (freely translated): ‘The duty to identify UBOs can usually be met by having the client declare who the UBO is.’; DNB Q&A and Good Practices, Q 3.17.

[22] EBA, Guidelines on revised ML TF Risk Factors, (2021), p. 41: ‘Firms should be mindful that using information contained in beneficial ownership registers does not, in itself, fulfil their duty to take adequate and risk-sensitive measures to identity the beneficial owner and verify their identity. Firms may have to take additional steps to identify and verify the beneficial owner, in particular where the risk associated with the business relationship is increased or where the firm has doubts that the person listed in the register is the ultimate beneficial owner.’

independent source as recommended by DNB in its AML Act Guidance.[23]

For non-Dutch low and medium risk customers the Industry Baseline proposes UBO identification relying on either (a) the UBO-declaration by the customer; or (b) by relying on other reliable sources such as foreign government maintained repositories. For high-risk non-Dutch customers banks are (i) to rely on the UBO-declaration by the customer; and (ii) supported by further information such as a register of shareholders or a trust deed. Unmistakably, banks will be greatly facilitated in their identification of foreign UBOs in this manner. However, one might question what the true effect will be of this identification procedure, where it is solely up to the customer to deliver honest input on the identity of the UBO, emphasised by the juxtaposition included in the Industry Baseline of either (a) input from the customer or (b) reliance on other reliable sources. Admittedly, these other reliable sources are often the product of information collected from the customer in one way or another. Nevertheless, the approach to both Dutch and non-Dutch customers does make the Terugmeldplicht of art. 10c AML Act a dead letter as no malicious customer will make a notification that the information included in the UBO excerpt is incorrect.[24] In the long run this might also endanger the identification on the basis of the UBO-register as the integrity of the data included in the register might become controvertible.

For verification the Industry Baseline recommends that low and medium risk customers' UBOs are verified using the information obtained in the identification phase and alternatively that an (un)verified copy ID is requested to add a slightly more intensive screening. High-risk customers' UBOs' identity are always to be verified using at least some form of additional documentation such as a certified copy of the identification document of the individual(s) concerned. For low and medium risk companies the verification thus resides in requesting the customer to verify the UBO information included in the UBO-register and potentially an unverified copy ID. This again seems to be a tight balancing act with the AML Act as art. 3(15) AML Act dictates that verification of the identity of the UBO cannot solely be done on the basis of the UBO-register.[25] Nevertheless, DNB supports the approach forwarded by the NVB, albeit only explicitly within the perimeter of SDD and low-risk customers.[26]

[23] See for example a case where a Dutch district court rejected the sole reliance on a singular excerpt from the trade register for UBO identification, and even more for verification, District Court Rotterdam, DNB/Bunq, 14 August 2023, ECLI:NL:RBROT:2023:7380, r.o. 17 and 21.

[24] rovided that in cases where a notification to the FIU is made pursuant to art. 16 AML Act no terugmeldplicht exists.

[25] See also DNB, AML Act Guidance, p.37: 'Verification cannot be done solely on the basis of the extract obtained. An institution should always verify the identity of the UBO, regardless of the risk.'

[26] DNB Q&A and Good Practices, Q 3.17 and GP 3.11.

Moreover, the AMLD4 amended the risk-based requirement to perform a verification of the UBO's identity with a hard requirement that can be performed in a risk-based manner.[27] A further question that could be raised is what happens to the obligation to make the ownership structure of customers clear for the obliged entity pursuant to art. 3(2)(b) AML Act.[28] If the bank is still to obtain clarity on the legal structure, which is also closely related to identifying the purpose and nature of the business relationship, then it would have to request additional information from the customer or utilise an alternative (proprietary) database to obtain this data, thus possibly reducing the gains of the Industry Baseline. DNB considers that the depth of the investigation of the ownership structure of a customer must be proportionate to the complexity and the risk of the structure.[29] Although seemingly purporting a risk-based approach, it is difficult to understand how an investigation can be risk-based but also linked to the complexity. Either a structure is complex and the obliged entity will have to fully explore it, or it is not and the UBO shall be easily identified. It seems that the complexity of the ownership structure shall therefore be the driver of the depth of the investigation, where a risk-based approach may be taken in respect of its outcomes.[30]

[27] TK 2017-2018, Kamerstukken 34808 Nr. 3, p. 48 (freely translated): 'In line with the fourth anti-money laundering directive and the FATF recommendations, it was chosen to always change "risk-based and adequate measures" to "reasonable measures". The wording "risk-based, adequate measures" indicated that the obligation to verify the identity of a UBO focused on those cases where, in the institution's judgment, there was a higher risk of money laundering or terrorist financing. The fourth Anti-Money Laundering Directive leaves no room for this interpretation. By replacing the aforementioned formula with "reasonable measures", it makes clear that an institution must at all times make efforts to verify the identity of a UBO as part of the customer due diligence process.'

[28] As also obliged by art. 13(1)(b)AMLD4.

[29] DNB Q&A and Good Practices, Q 3.15.

[30] DNB Q&A and Good Practices, GP 3.8-3.9.

4.
PSEUDO UBO
INDUSTRY BASELINE

4. PSEUDO UBO INDUSTRY BASELINE

The third Industry Baseline sees to the residual category of UBOs known as 'Pseudo UBOs' following a failure to identify a UBO by the factual control criterion or ownership criterion.[31] This fallback category of UBO is provided for in art. 3(1)(a)(2) Implementation Decree AML Act (*Uitvoeringsbesluit Wwft 2018* '**AML Act Decree**') and shall pursuant to the Industry Baseline be established as the statutory members of the executive board (or executive partners) (the '**Senior Management Official(s)**') at the customer level, which is not necessarily always, but may (and shall often) coincide with, the ultimate parent holding company.[32] As EU trade registers have third-party effect, they shall be able to be relied upon as sufficiently reliable sources for the identification of the pseudo-UBOs in low and medium risk cases according to the NVB. In high-risk instances, the customer shall also have to be requested to provide the identity information of the relevant Senior Management Official(s).[33]

Concretely, a bank shall have to record in the file of an EU customer that (i) Senior Managing Official(s), being the statutory executive directors or partners, are identified as UBOs as a fall-back after exhausting all other possible means to identify the UBO and (ii) that there are no grounds for suspicion of ML/TF. For high-risk EU customers, a bank shall furthermore have to request the customer to confirm the statutory executive directors (or executive partners) which shall have to be recorded accordingly.[34] For non-EU customers, banks shall have to request the customer to (i) provide the names of the Senior Management Officials, i.e. executive board members, (ii) the identities of the Senior Management Officials and (iii) that the pseudo-UBOs are being recorded as fallback solution, as well as that there are no grounds for suspicion of ML/TF (in low and medium risk cases).

Verification of the identity of the pseudo-UBOs can be performed based on the information included in the trade register excerpt, open sources or information provided by the customer. Alternatively, banks can request the pseudo-UBOs to provide a copy of their identity document. For high-risk cases, bank shall have to perform verification of the identity using a verified copy of an information document provided by the customer. Similar objections as with the (lack of) verification of the UBO as detailed under paragraph 1.2 can be raised here, with the actual verification in low and medium risk cases being a semantical differentiation that in

[31] NVB, Risk-Based Industry Baseline: Pseudo UBOs, (2023).

[32] As also determined in art. 3(6)(a)(ii) AMLD4.

[33] DNB Q&A and Good Practices, GP 3.13.

[34] However, a certain ML/TF suspicion shall exist given the high-risk status and thus recording of the absence thereof, which is requisite in medium and low risk cases, shall be able to be foregone.

practice will not be able to be delineated nor differentiated from the identification of the pseudo-UBOs.

It remains crucial that any and all use of the pseudo-UBO shall only be that of an ultimum remedium in ascertaining the UBOs failing the possibility to do so via the factual control or ownership criteria. Any and all use of the pseudo-UBOs shall be properly documented by the obliged entity.

5.
CUSTOMER DATA ACTUALISATION INDUSTRY BASELINE

5. CUSTOMER DATA ACTUALISATION INDUSTRY BASELINE

This Industry Baseline seeks to clarify and streamline the cumbersome task of banks to keep a complete, accurate and up-to-date set of data regarding their customer relations pursuant to art. 3(11) AML Act.[35] Underlying the Industry Baseline are the four principles of: (i) completeness of data, requiring banks to ensure that they have a full range of necessary, obligatory, information available in their databases; (ii) correctness of data, which requires banks to have correct data recorded, which shall be presumed to be the case unless that bank has received an indication that the data recorded is incorrect; (iii) risk-based approach, which according to the Industry Baseline will allow banks to differentiate between the risk sensitivity of certain data points, f.i. the name of the customer versus the ID-document number, and the measures applied to ensure correctness and completeness; and (iv) sources, relating to the origin of data used by banks, which preferably shall be done with a minimal level of customer interaction in order to improve user experience.

The Industry Baseline specifically sets out to determine the range of customer data in scope, the moments of data actualisation, the methods thereof and sources that can be used for data actualisation, thereby attempting to demonstrate the effective implementation of a risk-based customer data actualisation process. On the whole, the Industry Baseline purports to reduce the amount of interactions with the customer and similarly purports to reduce the intensity of the data actualisation process without, at least such is the intention, infringing on the effectiveness of the process. Similar to the previously discussed Industry Baselines, the risk-based approach is interpreted to mean that when banks clearly differentiate between low medium and high-risk information they can (generally) apply a toned-down screening process that has been adjusted to the respective risk levels, where emphasis shall be put on higher-risk data points such as country of residence.[36] The Industry Baseline does not address SDD[37] or EDD cases, yet it would be interesting to relate the risk-based approach to datapoints with the obligation to ensure proper data actualisation included in art. 8(11) AML Act. Surely this provision shall not be able to be interpreted to entail the same risk-based approach as art.

[35] Being the implementation of art. 14(5) AMLD4.

[36] NVB, Risk-Based Industry Baseline: Client data actualisation, (2023), p. 6: 'For their risk-based client data actualisation banks should consider the risk relevancy of client data for risk assessments. Example: to determine high risk jurisdictions, the country of residence is more relevant than the city or street name of the client. As a result, a bank may choose to have a lower risk appetite to incorrectness of the country of residence compared to other parts of the residential address. Therefore, the bank might continuously monitor for changes in country of residence but might not ask the client to periodically confirm the address.'

[37] See the DNB Q&A and Good Practices, paragraph 3.3. Even in cases of SDD, the obliged entity shall be held to perform a risk assessment where it shall not be able to mechanically rely on the low-risk nature of its customer. Actualisation of customer data may be at a lower frequency but shall not be able to be foregone.

3(11) AML Act as it concerns EDD. In that case, will certain information be high-risk due to the application of EDD, or is all data suddenly earmarked as high-risk as it concerns a high-risk customer? In other words, could it be acceptable that the data of a high-risk customer is not correct or complete?[38] Further questions could be posed as to the strong reliance of the NVB on the phrase risk-based in relation to the obligation to ensure data actualisation in whatever form is done. The AMLD4 removed the previously existing leeway in the AML Act where risk-based and reasonable measures was reduced to reasonable measures.[39]

The Industry Baseline propagates a preference for a trigger-based actualisation method rather than a periodically performed screening, or a combination of the two for that matter. Such a trigger-based screening, in principle permitted by DNB,[40] where banks shall be able to assume that data is correct until there are reasons to doubt the correctness of such data will ease the burden to continuously perform onerous revisions of the CDD database whilst lowering the amount of interactions with the customer.[41] From an operational point of view, such changes are only to be welcomed by the overworked compliance departments who shall be able to dedicate more time to the initial assessments and the high-risk cases, rather than performing repetitive re-screenings as a matter of routine without indications that there is a rationale to do so. This interpretation of the at least trigger driven screening seems to connect to the intention of the Dutch legislature with art. 3(11) AML Act, and the interpretation of DNB insofar that this is the very base scenario.[42] Banks will be required to have strong procedures in place to ensure proper identification of triggers for rescreening in order to warrant the effectiveness of the data actualisation, since non-detection of triggers does not acquit the bank from the obligation to act on those triggers. The risk-based approach only extends to the performance of the data actualisation, thus if a situation arises where no triggers are detected, be it legitimately or not, no-rescreening occurs and thus a bank would be in violation of the AML Act. Consequently, some form of periodic re-screening is, according to DNB, inevitable at least for high-risk customers, and perhaps also in particular for low-risk customers who shall generally not produce

[38] Seemingly not according to Recital (24) of the AMLD5, Directive (EU) 2018/843: 'The approach for the review of existing customers in the current framework is risk-based. However, given the higher risk of money laundering, terrorist financing and associated predicate offences associated with certain intermediary structures, that approach might not allow for the timely detection and assessment of risks. It is therefore important to ensure that certain clearly specified categories of existing customers are also monitored on a regular basis.'

[39] See note (14).

[40] DNB Q&A and Good Practices, paragraph 4.2 and GP 4.40.

[41] DNB Q&A and Good Practices, Q 4.35: 'The entity must take reasonable measures to keep the customer's records up to date. The customer file must be updated in any case if there is a relevant change to the customer's circumstances. This includes conspicuous and anomalous transactional behaviour as well as changes to the customer's ownership or control structure. Signals the entity receives from, for example, the customer themselves or the press and legal cases also qualify as relevant changes.'

[42] TK 2018-2019, Kamerstukken 35245 Nr. 3, p. 35.

many triggers.[43] The future AMLR also requires a minimum periodic rescreening of once every five years and a requirement to ensure that the data, information and relevant documents related to the customer stay up-to-date, see art. 21(2) AMLR. Additionally, the AMLR includes a new rescreening trigger in the event the relevant facts pertaining to the customer change, art. 21(3)(c) AMLR, which does not seem to align with the risk-based data actualisation procedure created in the Industry Baseline. The approach that is to be taken with regard to the majority of the customers (i.e. which qualify as medium-risk), remains undecided by DNB. However, it must be noted that DNB, unlike the NVB, does not necessarily open the door for a sole event-driven review with respect to these customers. At a very minimum, an obliged entity will have to include the frequency of screening in a policy ex ante, where we consider it to be the better view that medium-risk customers should be subjected to some form of periodic review.

Customer Data – Natural Persons

External recources	Internal Analysis	Customer Outreach
Customer & representative	**Customer & representative**	**Customer & representative**
• Name(s) (first + middle + last)**	• Name(s) (first + middle + last)	• Name(s) (first + middle + last)*
• Date of birth**	• Date of birth	• Date of birth*
• Residential address*	• Residential address**	• Residential address*
• ID doc: type, number, date, place**	• ID doc: type, number, date, place	• ID doc: type, number, date, place*
Customer:	**Customer:**	**Customer:**
• Purpose & nature	• Purpose & nature**	• Purpose & nature*
Representative:	**Representative:**	**Representative:**
• Mandate representatives**	• Mandate representatives	• Mandate representatives*

The sources that can be used for data actualisation are (i) external sources, such as proprietary databases; (ii) internal analysis, research done by the bank itself; and (iii) customer contact and outreach. The Industry Baseline reflects a strong preference for sources (i) and (ii) with as little possible recourse to the customer. This should achieve a situation where customers will be less frequently presented with a request for information, which should enhance their overall service experience.[44] Below a table is included that provides an indication of the preferred methods and sources to actualise data (**), other possible sources (*) and impossible sources (no *).

[43] Even more so if the expiry of a document is not to be regarded as a trigger as forwarded by the Industry Baseline and as seemingly supported by the parliamentary history: 'The obligation [of data actualisation red.] refers to keeping data up to date, not replacing (copies of) documents. For example, it is not intended that a copy of an identification document should be replaced when its validity has expired.' TK 2011-2012, Kamerstukken 3238 Nr. 3, p. 14. DNB Q&A and Good Practices, GP 4.40.

[44] DNB Q&A and Good Practices, Q 4.36 and GP 4.40.

Customer Data – Legal Entities

External recources	Internal Analysis	Customer Outreach
Customer: • Legal form** • Statutory name** • Trade name(s)** • Street, number and city of registration + country of incorp.** • Registration number** • Purpose & nature • Ownership and control structure**	**Customer:** • Legal form • Statutory name • Trade name(s) • Street, number and city of registration + country of incorp. • Registration number • Purpose & nature** • Ownership and control structure	**Customer:** • Legal form* • Statutory name* • Trade name(s)* • Street, number and city of registration + country of incorp.* • Registration number* • Purpose & nature • Ownership and control structure*
Representatives: • Name(s) (first + middle + birth)** • Date of birth** • Authority to represent customer**	**Representatives:** • Name(s) (first + middle + birth) • Date of birth • Authority to represent customer	**Representatives:** • Name(s) (first + middle + birth)* • Date of birth* • Authority to represent customer*
UBO: • Name(s) (first + middle + last)** • Size and/or nature beneficial relationship**	**UBO:** • Name(s) (first + middle + last) • Size and/or nature beneficial relationship	**UBO:** • Name(s) (first + middle + last)* • Size and/or nature beneficial relationship*
Additional for trust or other legal constructions: • Applicable law governing the trust or other legal constructions	**Additional for trust or other legal constructions:** • Applicable law governing the trust or other legal constructions	**Additional for trust or other legal constructions:** • Applicable law governing the trust or other legal constructions**

Source: NVB Risk-Based Industry Baseline: Customer data actualisation

Key to the effect of the Baseline is the application of a differentiated risk treatment of the data points listed in the table above with a corresponding periodic demonstration of the effectiveness of the data actualisation method applied by the bank. Banks need to be able to demonstrate that their chosen methodology for data actualisation, which is significantly liberalised by the Industry Baseline, is sufficiently effective in light of their risk appetite, their customers risk profiles and preferred service channels and that the information gathered in the update is effectively transposed into the CDD policies, procedures and files.[45] In the review, be it periodic or event driven, the obliged entity shall:

[45] DNB Q&A and Good Practices, Q 4.38 and 4.40.

a Check for sanctions and politically exposed persons (PEPs). For high-risk customers, a “bad press” check is also warranted;

b Analyse customer transactions, checking:

1 Whether the transactions fit the purpose and nature of the relationship;

2 Whether the transactions are plausible given the origin of the funds used in the relevant business relationship or transaction;

3 Whether there are conspicuous transactions or transaction patterns (large amounts, unusually large cash transactions, amounts transferred immediately to another account, possible use of the accounts by third parties, unknown counterparties). Transactions that stand out and cannot be directly explained must be analysed in more detail. For the purpose of this analysis, further information should be obtained from the relevant customer if necessary, for example on the source of the funds;

c Update customer data, including UBO data;

d Update risk profile. This may affect the mitigating measures that need to be applied.

We believe that this demonstrability requires thorough drafting of policies and procedures in order to safeguard the more lenient CDD framework, this as the legal framework did not change and thus the same regulatory goals need to be achieved with a reduced intensity screening. By nature, such adjustments in the data actualisation process need to be compensated with a higher degree of motivation for such methodologies by the obliged entities.

6.

EXPECTED TRANSACTION PROFILE BASELINE

6. EXPECTED TRANSACTION PROFILE BASELINE

The ETP Industry Baseline describes the risk-based approach applied by Dutch banks in creating and using ETPs in pursuit of their ongoing CDD obligations of art. 3(2)(d) AML Act. The Industry Baseline provides for an overview as to when ETPs are appropriate, accompanied by more detail on risk relevancy, determining the actual ETPs, risk response and the demonstration of the efficacy of the implementation of ETPs.[46] As a very clear sign of the significantly different approach to ETPs compared to that currently prescribed by DNB, the Industry Baseline notes that the 'DNB Leidraad is to be used as a good practice and does not represent minimum requirements.'[47] With the new presentation of the DNB Guidelines as DNB Q&A and Good Practices, this attitude of the Industry Baseline seems to be supported by DNB itself.

ETPs can, but according to DNB do not have to,[48] be used as a tool in both transaction monitoring and Ongoing Due Diligence ('**ODD**') and serves to identify deviating transactions that do not fit the expected transaction pattern of the customer, or the peer group in which the customer has been categorised by the bank. Already in 2006 a norm was included in the Dutch Decree Prudential Rules (*Besluit prudentieel toezicht Wft* '**DPR**') which entailed that an obliged entity should regularly check whether the transactions made by a customer are still logical in comparison to the original profile of the customer at onboarding.[49] ETPs have a difficult relationship vis-à-vis the overall risk profile of the client. ETPs help establishing the risk profile and shall be able to serve as a monitoring tool during the ODD phase.[50] In our view, DNB does not truly succeed in differentiating the two concepts and a situation where the ETP will significantly differ from the risk profile is hard to imagine. Therefore, we also struggle to imagine a situation where an obliged entity would not produce an ETP, as most likely it will already have done so in shaping the risk profile. The DNB Q&A and Good Practices seem to be somewhat at odds with itself, and possibly the AML Act. What probably is intended here, is that an ETP does not necessarily has to operationalised to the extent where it would aid in generating alerts.[51]

[46] NVB, Risk-Based Industry Baseline: Expected Transaction Pattern, (2023).

[47] Idem, p. 2.

[48] DNB Q&A and Good Practices, Q 4.6.

[49] Current art. 14(4) DPR, Staatsblad 2006/519, p. 109.

[50] DNB Q&A and Good Practices, Q 3.54 and GP 4.20.

[51] As also recognised by DNB Q&A and Good Practices, GP 4.15.

It is important to delineate rule-based transaction monitoring from ETPs as they do not necessarily entail the same purpose or process. Rule-based transactions monitoring uses pre-determined scenario's, commonly referred to as business rules.[52] Matches between transactions and such scenarios, also known as hits, are produced when a transaction presents a certain resemblance to instances of fraud or ML/TF whereas with an ETP a hit is produced because the transaction does not seem to fit the expected behaviour of that customer (or peer group of customers) and may, consequently be an indication of being a suspicious transaction (whether fraudulent or AML/CTF driven). The factual differentiation between these elements might be slim, especially in cases where banks use increasingly advanced methods such as artificial intelligence deployed on customer level to produce new business rules or to refine the ETP of said customer (or sub-group of customers).

The Industry Baseline aptly remarks that ETPs can have several purposes such as (i) to assess significant deviations of customer behaviour in comparison with the customer group's ETP; (ii) deviating behaviour can be relevant background information when performing customer risk assessments or handling alerts' (iii) as a safety net that could identify undetected cases of ML/TF or fraud after the transaction monitoring process; and (iv) as a tool to further refine ML/TF screening processes.[53] Furthermore, an ETP might serve as a trigger for updating the customer data as referred to in the Customer Data Actualisation Industry Baseline.[54]

There is no set method for establishing the ETP of a customer or of a peer-group of customers, although DNB does provide some generic guidance on this.[55] It is, furthermore, not obligatory to create customer specific ETPs, for as long as the ETP is sufficiently sensitive to be able to inform on unusual or unfitting transactions of a relatively homogenous group of customers. We appreciate that this is an increasingly difficult process given the increasing personalisation of finance, where the highly customer specific range of products and services used nowadays is far removed from the standard bank customer of the past.

It shall be a risk-based approach on which banks ascertain their customer's ETP, which, according to the Industry Baseline, shall not have to be recorded in the CDD file of each and every customer. This latter statement could be disputed as comparing the ETP ex post requires some assumption as to what the ETP was ex

[52] DNB Q&A and Good Practices, GP 4.2-4.5. The business rules can be based on factors such as (i) the type of client; (ii) the category of client (e.g. private, retail or professional); (iii) client risk profile; (iv) country concerning the transaction; (v) the product or service involved; (vi) the distribution channel (e.g. physically or online); (vii) the nature and frequency of the transaction; (viii) international transactions being remitted; and (ix) the SIRA.

[53] Id at 25, p. 5.

[54] Id at 11, p. 56.

[55] DNB Q&A and Good Practices, Q 4.7 and GP 3.44 - 3.45.

ante, in other words, some record of the ETP of the customer needs to be maintained and the CDD file seems to be the logical place for this.[56] This view seems to be supported by the EBA and DNB.[57] ETPs can be based on characteristics of the customer involved, either legal or natural persons, such as age group, residency, industry, customer size, type of products obtained from the banks etc.. As indicated before, it may not be possible, or feasible to create ETPs for each individual customer wherefore it is logical that a risk-based approach might be taken to allocating ETPs to customers or groups of customers, the prior referenced peer groups. Although not a 100% fit of the customer with a peer group ETP shall be mandatory, it is necessary that the chosen ETP remains somewhat indicative of the expected behaviour pattern of the customer. Again, a risk-based approach where low and medium-risk customers need a less bespoke approach than the high-risk customers may be taken. If a peer group does not seem to align with the actual behaviour of the client, it shall be reassigned, or if the misalignment persists, the ETP itself shall be adjusted.[58]

The Industry Baseline stresses the importance of banks being able to show the effectiveness of their AML/CTF measures, including their use of ETPs. Instrumental is that the description of the measures taken as described in the Systematic Integrity Risk Assessment ('**SIRA**') are sufficiently substantiated and substantiating the ETP measures as deployed by the bank. Documentation plays an important role in this process, where all judgement calls of an obliged entity on the adequacy of the AML/CTF measures taken need to be underpinned with methodologies, evaluations and testing recorded in a durable manner. The Industry Baseline goes on to reiterate the standpoint of the Wolfsberg group, an association consisting of the largest banks in Europe, that if a bank finds its controls to be ineffective, e.g. ETPs, then it should consider eliminating it so as to enable the redeployment of the resources elsewhere.[59] This approach seems problematic to align with the legal obligation of art. 14(4) DPR or the, admittedly indirect, obligations to create business profiles of customers by which the expectedness of a given transaction can be assessed included in art. 14(5) AMLD4 and art. 16(5) jo. 21(1) AMLR.

[56] In its guidance for Post-event Transaction Monitoring Processes for payment service providers, DNB also states that the ETP should be recorded in the customer's CDD file, see DNB, Post-event transactiemonitoringsproces bij betaaldienstverleners, (2017), p. 12. See also District Court Rotterdam, DNB/Bunq, 14 August 2023, ECLI:NL:RBROT:2023:7380, r.o. 24.

[57] Id at 11, paragraph 4.77.

[58] DNB Q&A and Good Practices, GP 3.44.

[59] The Wolfsberg Group, Demonstrating Effectiveness, (2021), p. 4: 'Where a control requires significant time and/or resources for minimal risk mitigation, FIs should consider changing or eliminating the control altogether and reallocating those resources to those with demonstrably more effective outcomes.'

7. ONGOING DUE DILIGENCE INDUSTRY BASELINE

7. ONGOING DUE DILIGENCE INDUSTRY BASELINE

ODD often proves to be an elusive concept that requires significant investment of time and resources with sometime seemingly little outcome. The ODD Industry Baseline provides for a framework that can, in principle, be applied to all customers regardless of their risk qualification. The risk-based approach presented in the Industry Baseline provides for an ODD process that mainly focusses on an event driven review instead of cumbersome periodic reviews. The thought here being that periodic reviews do not necessarily add much risk sensitivity as they are not receptive to actual risks being present. Instead an event driven process should ensure that the ODD obligation shifts towards a risk-oriented framework where the exercise undertaken is always done in response to a trigger, thus theoretically always providing a relevant outcome. Periodic reviews are comprehensibly rejected by this Industry Baseline, fully tilting the ODD process towards event driven reviews, which can be considered somewhat at odds with the obligation of art. 3(2)(d) AML Act and the seemingly hybrid model as purported to be established in art 22 AMLR.

An event driven ODD process leans on three core elements: (i) customer data (see paragraph 5 above); (ii) alert and event generation (see paragraph 8 below); and (iii) alert and event handling. The third element is the core of the Industry Baseline and is sub-divided into three risk-based categories: (a) automated handling of events and alerts without human intervention; (b) a risk-differentiated alert and event handling, primarily conducted by a human; and (c) the comprehensive review by a human. The alerts triggering the event driven reviews are all created by a fully automated alert generation process which will be discussed in further detail below, yet we note here that this initial triage of events by a detection mechanism, i.e. model, is quintessential for the proper performance of the ODD process. Truly the mantra garbage in garbage out applies here as a poorly designed and controlled detection mechanism will obfuscate the entire ODD process. The Industry Baseline is recognisant of this and puts a large emphasis on an adequate governance surrounding the model, to be refined with the Industry Baseline on the models in alert and event generation (paragraph 8), however, actual concrete governance guidance is absent (in this Industry Baseline), with DNB not providing much guidance either.[60]

[60] A topic somewhat related involves the governance requirements surrounding the use of artificial intelligence that will be obligatory under the proposed EU AI Act. The many layers of complexity and the high reliance on the model can on the one hand be encouraged as data intensive tasks such as ODD are highly suited for AI applications. On the other hand, self learning customer monitoring models that determine new EDR triggers and consequent risk responses seems to be a fragile chain prone to biased decision making that might prove surprisingly stubborn and difficult to address.

The risk-based alert handling relocates the vast majority of alerts to automated decision making or a marginal assessment of the AML/CTF analyst through a risk-differentiated procedure. In these processes the alerts or events generated are befitting of the ETP, customer data and risk profile created of any customer and thus can generally be addressed by an automated risk response. Alternatively, the AML/CTF analyst is instructed to solely focus on the part of the alert that has not already been incorporated in the customer's risk profile somehow.[61] The Industry Baseline gives the example of a customer that pursues a cash-heavy high risk business from the Netherlands with a high-risk third country. These factors have been incorporated in the CDD framework surrounding that customer. If a customer is for example also showing transaction data in Belgium which geographical location has not been incorporated in the customer's CDD profile. The analyst is instructed in a risk differentiated review to focus on the business activities in Belgium and not on the 'duly' covered high-risk activities in the Netherlands. If the analysts considers there to be sufficient reason to do so, a comprehensive review may be triggered where the entire CDD dossier is reviewed. The rules by which a CDD-analyst is to ascertain what level of scrutiny is to be applied must be described in an alert handling policy.[62] DNB reiterates the difference between alerts and unusual transactions by stating that it is up to the CDD-analyst to conclude whether an alert constitutes an unusual transaction and thus needs to be reported to the FIU.

Undoubtfully, if all processes are perfectly shaped, such risk-based alert handling covers the most acute risks and could be a risk-based implementation of the AML Act. It seems, however, that the proposed framework lacks sufficient reflective ability as risks that are considered to have already been addressed are surpassed.[63] Comparing this to the Data Actualisation Framework where it was stated that for low risk customers data might only be updated when the bank receives a prompt to do so, there seems to be a potential for a blind spot where data is not updated because the customer does not trigger EDRs, not unthinkable for high-risk customers with well developed ETPs/risk-profiles who are not expected to produce many EDRs as this would be an indication of an improper initial CDD set-up.[64] Or in the case where a malignant customer would intentionally avoid surpassing certain

[61] DNB Q&A and Good Practices, GP 4.23.

[62] DNB Q&A and Good Practices, GP 4.22-4.24.

[63] A thought that could be had is that per this, in principle not unreasonable logic, the risk-differentiated treatment would produce an inverted risk-based alert handling process. Assuming high-risk customers were dealt with comprehensively in the initial CDD phase, they will generate relatively few alerts outside of the ETP, customer data and risk profile of that customer as compared to low-risk customer where all alerts generated will most probably be outside of the expected behaviour per se. Under the risk-differentiated review this would mean that low-risk customers are subject to a more intense review than high-risk customers, leading to issues such as data actualisation, as the high-risk customers might be revisited less frequently in an risk-differentiated EDR.

[64] The risk-based data actualisation requirements of the AML/CTF Guidelines of the Minister of Finance where 'The higher the risk posed by a client, the more frequently customer due diligence data should be updated' would be jeopardised by 'too good' initial CDD as such customer ought not to produce many alerts or events that are outside of the bank's expectations for that customer.

thresholds, for instance by means of structuring or smurfing.[65] A low-risk customer, might trigger only alerts that are to be covered by automated case handling and risk responses – potentially being hibernation, i.e. no action whatsoever or no human assessment.[66] The Industry Baseline does state that if automated events start to accumulate such might also be a trigger for a comprehensive review in and of itself, although such an approach may lack sufficient retrospective ability as an alert will only be generated contingent on a future uncertain trigger. However, the mere labelling of a customer risk profile with one or several hibernation risk responses will most likely not be compliant with the obligation to perform ODD, as also confirmed by DNB: 'Every alert should be assessed. An obliged entity may not run the risk that an unusual transaction shall remain undetected, and that such transactions are not notified to the FIU.'[67] Therefore, DNB requires a strict governance of automatic alert handling systems, where the automatic responses shall at least periodically have to be reviewed.[68]

[65] DNB Q&A and Good Practices, GP 4.16.

[66] The lack of which might be contrary to art. 35 AML Act.

[67] District Court Rotterdam, DNB/Bunq, 14 August 2023, ECLI:NL:RBROT:2023:7380, r.o. 23-24; DNB Q&A and Good Practices, paragraph 4.1.4.

[68] DNB Q&A and Good Practices, Q 4.18.

On the whole an automated system will be a pattern most befitting to the average customer CDD profile, however, it is not the average customer the AML/CTF framework is designed to address. It is the malignant parties that may exploit these blind spots specifically targeting them and thereby evade human scrutiny. While it is no given that human scrutiny is superior to that of an automated system, most probably a human is better able to detect slight hints of unusual behaviour that have taken place (mostly) within the ex ante limits set. It is such behaviour that might be detected by non-event driven periodic reviews whilst event driven reviews are only as good as the triggers prompting them.[69] To that end, the Industry Baseline requires at least the following operating conditions to be met:

a Adequate processes for the continuous improvement of data quality, whereby banks strive for their relevant customer data to be complete and correct (see also paragraph 5);

b Automated risk detection mechanisms and alert and event generation must be in place (based on transaction patterns, customer behaviour and changes in customer or transaction data) and have been proven effective;

c Risk triggers should effectively cover the potential risks within the bank's customer portfolio and the bank's risk assessments, i.e. the ODD framework should be risk-sensitive;

d Ensure compliance with regulatory requirements, which at times may be threatened by a too heavy reliance on a risk-based approach;

e Ensure adequate design and implementation of event driven review processes and adequate operational effectiveness of those (see paragraph 8);

f Ensure adequate oversight on effective event driven review processes; and

g Alerts or events will be processed within the relevant timeframe in accordance with the risk appetite.

[69] DNB Q&A and Good Practices, Q 4.32: 'A (periodic) review is of the essence to determine whether certain business rules or models unjustly did not produce any alerts and whether adjustments are therefore necessary.'

8. MODELS IN ALERT AND EVENT GENERATION INDUSTRY BASELINE

8. MODELS IN ALERT AND EVENT GENERATION INDUSTRY BASELINE

Arguably the most relevant and state-of-the-art Industry Baseline, the Models in alert and event generation Industry Baseline (the '**Model Industry Baseline**') provides a much-needed guidance on the backbone of the risk-based AML/CTF framework in place at banks: the use of complex detection systems. These systems referred to as 'models'[70] are widely adopted by (Dutch) banks for AML/CTF purposes and are perfectly allowed under the technology agnostic AML Act, although they are not required according to DNB.[71] With the burden of the AML/CTF process increasing due to the rising number of digital payments made by (Dutch) bank customers automated systems are the only real possibility to handle – at least the initial identification of – ML/TF risks. Yet a high degree of uncertainty surrounds AML/CTF models as no subject specific supervisory guidance exists, albeit that DNB in 2019 published the highly useful 'SAFEST' principles for the use of AI by financial institutions.[72] Approaches to model programming generally stem from programmer knowhow and market experience leading to low comparability of approaches and repeating high costs for each institution having to devise a new system whilst simultaneously assessing whether it is compliant with the AML Act.[73] To further exacerbate these complications, DNB prohibits the use of 'of the shelf' models if these are not tapered to the specific profile of the obliged entity.[74]

The Industry Baseline analyses several use cases for the deployment of models for AML/CTF purposes such as: customer filtering, transaction filtering, transaction monitoring, customer monitoring and event and alert handling triage. In other words, virtually all topics discussed above may involve some form of application of models, and similarly the Industry Baseline describes a wide range of types of models that can be used for an equally wide range of applications. The paradigmatic application of the models described in the Industry Baseline is not that revolutionising nor interesting as it mostly connects to instances of model applications referenced in other Industry Baselines or it follows common sense. For example, the quantification of ML/TF risks into low, medium and high buckets with corresponding alert handling/data actualisation or CDD measures all feel fairly intuitive. We therefore refer to the Industry Baseline for the concrete use cases

[70] See for the definition of models used in the Industry Baseline: Board of Governors of the Federal Reserve System Office of the Comptroller of the Currency, Supervisory Guidance on Model Risk Management, (2011).

[71] DNB Q&A and Good Practices, Q 4.3 and 4.11.

[72] DNB, General principles for the use of Artificial Intelligence in the financial sector, (2019). These principles have had a tremendous influence on the use of AI in the EU financial sector, yet it must be acknowledged that although containing universal principles, a four year old general document is hardly concrete guidance on a rapidly developing subject as RegTech.

[73] This latter exists only in a limited form as models are traditionally one of the most closely guarded secrets of banks.

[74] DNB Q&A and Good Practices, Q 4.5.

that are suggested but reiterate the statement that the current transition from rule-based models to advanced models[75] is one that is, also according to DNB, only to be supported.[76]

The added value of the Industry Baseline is in the governance framework surrounding the use of models, which emphasises accountability and demonstrability of the effectiveness of the models, which is reverberated in the DNB Q&A and Good Practices.[77] Statements that the use of model, or more broadly automated systems, requires sufficient explainability and efficacy have been included all over the Industry Baselines yet have been relatively poorly developed. Ultimately such qualitative judgements are reserved for the supervisory authorities and the banks themselves as they have to decide what is their measure of the risk-based approach and how they deem it to be fitting to their risk appetite. The Industry Baseline does provides some clear requirements that model risk management frameworks should at least outline:

a Standards for ownership of and responsibilities and accountability for models (e.g. an overview of competent bodies or functions and their decision making processes and procedures);

b Requirements and standards for (metrics of) model performance, fairness, and explainability;

c Requirements and standards for model monitoring;

d Requirements and standards for data quality management and data governance;

e Requirements and standards for the technical infrastructure in which models operate;

f Requirements for training and awareness for stakeholders;

g A process for managing model development and modification, including testing, validation, and approval before implementation;[78]

h Model documentation standards;[79] and

i Policies that describe the model approval and risk acceptance procedures.

[75] Advanced models generally being a model driven by more advanced technologies than traditional data crunching algorithms, such as self-learning AI or other forms of AI. The use of AI is recognised as a good practice for more complex obliged entities by DNB, DNB Q&A and Good Practice, GP 4.1.

[76] DNB Q&A and Good Practices, GP 4.15.

[77] DNB Q&A and Good Practices, Q 4.8.

[78] DNB Q&A and Good Practices, paragraph 4.1.6.

[79] The Industry Baseline here refers to a yet to be published Industry Baseline: the NVB Industry Baseline on 'Technical Model Documentation.'

These requirements are largely derived from the previously mentioned DNB 'SAFEST' principles and also seem to be inspired by the forthcoming EU AI Act yet their quasi endorsement by DNB do make these requirements concrete indications as to how model governance should be constructed in the Netherlands.[80] The Industry Baseline goes on to state that banks can use comparative performance analysis to identify the benefit of the advanced model over the old, rule-based model without having to show that the new model presents the same results as the old model. Such an approach would be innovation stifling as an improved model should not be expected to produce equivalent results as the old model, but superior results.

Recognising the need for additional governance, the Industry Baseline goes on to state the supplemental governance requirements necessary for the use of advanced models in ODD. Starting with a clear demarcation between responsibilities for the model, i.e. between the first-line AML/CTF compliance function or the model risk management function, both holding mandates to control and review the model, which should be clearly documented. Such documentation should, in line with the SAFEST principles, always indicate that the management board remains the final responsible party for the use of models. Once the general accountability has been sorted out, banks should:

a Determine and document the positioning of the model in their ODD framework;

b Have procedures in place to document and validate the risk coverage, which should provide an insight into the efficacy of the ODD model (on a management level);[81]

c Define model performance metrics that enable the objective comparison of models, e.g. for model selection or to detect deterioration of performance. Such metrics may, according to the Industry Baseline, eliminate the necessity for 'shadow' runs of the old model against the new model in parallel runs;[82]

[80] DNB Q&A and Good Practices, Q 4.32 et seq.; Yet it must not be forgotten that, in the words of the Industry Baseline itself: 'The [Industry Baseline] describes the application and execution of the risk-based approach, supported by models, in more detail. Thus, the Industry Baseline itself does not present the law nor direct supervisory guidance but a mere practical application in the eyes of the Dutch banks.

[81] The Industry Baseline further specifies: 'Banks should perform such coverage testing prior to implementation and during the use of the model. Specifically, banks should monitor if the risk coverage of the models is adequate and have procedures in place to follow-up on the discovery of new or missed ML/TF risks to enhance or adjust their control framework and safeguard that learnings are fed back to optimise or (re)develop existing models.' NVB, Industry Baseline on 'Models in alert and event generation', (2023), p. 8. We believe this to harbour the largest problem of model governance that has yet to be answered satisfactorily, how to monitor ex ante and medias res whether the model is function properly. The approach suggested by the Industry Baseline is a good start but omits the 'black box' problem or the 'inherent model problem' of it only being so good for as long as it is, as at the end of the day, a model is only a model and never 100% accurate (as also recognised by the Industry Baselines).

[82] Again, the to be published Technical Documentation Industry Baseline is referenced. It can be questioned to what extent the supervisory authority would agree to such elimination as in the absence of objective metrics defined by the supervisory authority themselves such non-compared metrics would lead to a high degree of required institution specific analysis and significant supervisory know how of the institutions processes.

d Decide, based on their SIRA and risk appetite, the minimum performance they require of each model; and

e Define requirements and standards for data governance that apply to models, where art. 3(11) AML Act imposes additional data actualisation requirements due to the AML/CTF application of the model.[83]

The DNB Q&A and Good Practices provide important guidance on the back testing of models, which should continuously inform the obliged entities on required adjustments to their automated systems.[84] As a minimum, an obliged entity shall be required to create a periodic feedback-loop that evaluates the efficacy, explainability and effectiveness of the models used.[85]

A problematic statement in the Industry Baseline is that advanced models do not require more stringent controls than traditional rule-based models. Whilst it is true that such does not always necessarily have to be the case, the majority of times the advanced model will have more autonomy or even decisional power transferred than the old model, perhaps even tacitly,[86] and thus requires stronger governance. This is the crux of the use of advanced (AI driven) models in the financial sector, or any sector, as human judgment is increasingly substituted for the (perhaps superior) judgement of an AI or model. The EU AI Act seeks to address exactly this problem, preventing the creation of so-called black boxes that no one can explain nor feel accountable for, or to. In the same vein, the Industry Baseline stresses the importance of transparency and the prevention of biased, perhaps discriminatory, decision making. Surely, a large step has to be made in the governance framework of advanced models to properly address these issues, in which the Industry Baseline and the DNB Q&A and Good Practices are a useful stride.

[83] Thus, data protection will also play a large role as the data processed is typically sensitive personal data for purposes of the GDPR.

[84] DNB Q&A and Good Practices, Q 4.33-4.44

[85] DNB Q&A and Good Practices, GP 4.30-4.34.

[86] If a self-learning customer monitoring model is deployed, for example, then an AI might develop indicators that in its view signal ML/TF risks whilst this reason for the inclusion of the indicator can be fully opaque to the model owners who see a well functioning indicator that was developed by the model. The nuance lies in the difference between the designation of the model and the perception of the human user.

9.

NOT-FOR-PROFIT ORGANISATIONS INDUSTRY BASELINE

9. NOT-FOR-PROFIT ORGANISATIONS INDUSTRY BASELINE

NPOs[87] play a vital role in many national economies and social systems. Their efforts complement the activity of the governmental and business sectors in providing essential services, and as such fulfil an essential role in society.[88] In practice, NPOs encounter difficulties when accessing the financial system due to factors inherent to their operations, such as the legal forms used (e.g. foundations), the often difficult geographical locations they are active (e.g. conflict jurisdictions) and large scope of contributors, all of which could be construed as high-risk indicators as included in Annex III to the AMLD4. Therefore, NPOs are often de facto considered to present a high AML risk, requiring application of the EDD measures of art. 8 AML Act and consequently NPOs are regularly exposed to de-risking practices of banks,[89] with anecdotal evidence of a minimum of three months necessary to open a payment account for a foundation.

Both the former DNB Guidance and the DNB Q&A and Good Practices remain mostly silent with respect to NPOs, with most of the existing guidance to be found in EBA guidance and FATF Recommendation 8, including the explanatory notes related thereto. The NPO Industry Baseline is therefore highly relevant to ensure that the social function of NPOs is not unproportionally hindered by an inadequate interpretation by obliged entities of the requirements stipulated under the AML Act and/or the AMLD4.[90]

The Industry Baseline reaffirms the (revised) position of the FATF that in principle a risk-based approach needs to be taken as to the CDD process of NPOs.[91] Given that many of the high-risk indicators of the AMLD4 may be applicable, it is a likely possibility that the NPO is identified as presenting a high-risk and therefore EDD must be applied. However, the Industry Baseline argues that a thorough investigation into the circumstances of the NPO will need to be undertaken, which contrary to other customers, most probably will require intensive customer contact. Of course, the level of intensity of these client communications shall be aligned with

[87] EBA, Amending Guidelines to the ML/TF Risk Factors Guidelines in relation to NPOs, (2023), p. 9: "Not-for-profit organisations' A not-for-profit organisation is a legal person or arrangement or an organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes.'

[88] FATF, Recommendations, p. 58.

[89] EBA, Opinion on de-risking, (2022); Not always unjust, for instance see: Gerechtshof Amsterdam, 28 December 2021, ABN Amro/ISOOK, ECLI:NL:GHAMS:2021:4148.

[90] NVB, Not-for-Profit Organisations Industry Baseline, (2023), p. 7.

[91] FATF, Public Consultation on the Revision of Recommendation 8 and its Interpretive Note, (2023): 'Countries should develop an understanding of the different degrees of TF risk posed to NPOs and of the corresponding different levels of mitigating measures they require. Many NPOs may face low TF risk exposure, may have adequate self-regulatory measures to mitigate such risks, and/or may already be subject to adequate level of legal and regulatory requirements, such that there may be no need for additional measures.'

the complexity and transparency of the NPO in question. For example, a large well known NPO supported by the UN may require a lower level of scrutiny compared to a newly established NPO that has no proven track record. Such procedure seems to require a high-risk approach to the initial screening, which is commensurate to the potential risk indicators, without prejudice to the actual risk profile of the NPO which may well be medium or low. This approach of focussing on the initial screening is aligned with that of the EBA in its Annex to the ML/TF Risk Factors Guidelines concerning measures for NPOs.[92]

[92] EBA, Guidelines on revised ML TF Risk Factors, (2021), p. 125-128.

Below we have included the table provided by the NVB containing both risk reducing and risk enhancing factors. We have supplemented this with the risk factors of the EBA and FATF insofar possible.

Risk Factors	Risk Reducing	Risk Increasing
Governance	• Legal form: religious organisation or an association, such as housing association, student association, sports club, hobby association, political association, industry association; • Legal form: foundation, only if: – statutes containing relevant standardised elements like transparency in ownership and executive control; and – transparent governance structures; and – pursuing philanthropic ends; • UBOs/senior managing officials residing in NL; • No (family) ties between board members other than business; • Clear governance and established management capabilities; • Demonstrated adherence to compliance policies, procedures and controls.	• Legal form: foundation (including STAK), such as: – complex and non-standardised statutes, or – non-transparent governance structures; • Limited or no binding with NL (e.g. composition of the board, purpose and nature of relationship with NL); • Absence of adequate internal compliance policies, procedures or controls.
Transparency	• Disclosure of financial statements; • Transparency of financial flows; • Publication of annual report;[93] • Independent audit report.	• No clarity on or insight into the origin and destination of financial flows; • No administration or financial reporting.
Reputation **Funding** **Geographies** **Transactions** **Objectives** **Industry Association**	• Positive track record; • No adverse media related to Financial Economic Crime or sanctioned activities.	• Linked to extremism, extremist propaganda or terrorist sympathies and activities; • Involvement in misconduct or criminal activities, particular related to Financial Economic Crime; • No or short (less than 12 months) track record.

[93] This risk indicator should be considered in context and may not necessarily be an indicator of low-risk ab ipso.

Risk Factors	Risk Reducing	Risk Increasing
Funding	• NL and EU governments and supranational bodies; • Membership fees; • Clear funding structures; • Sponsoring.	• Cash deposits and/or high denominations; • Donations substantially deviating from expected transaction behaviour; • Deposits in crypto-currencies; • Other deposits not channelled through the payment system.
Geographies	• EU; • Equivalent low risk geographies with an effective AML/CTF framework.	• Countries with sanctions (unless formal exemptions apply for humanitarian assistance/ basic human needs); • Countries on the FATF grey and black lists; • EC high risk third countries; • Including intermediations in HRTC through third-parties.
Transactions	• Transactions with established parties; • Proven track record; • Limited turnover in the account (e.g. annual less than EUR 100.000); • Transactions aimed at immediate emergency relief in humanitarian crisis situations under formal exemption (unless controlled by sanctioned persons/entities).	• Complex structured transactions (without logical explanation); • Unusual or excessive cash withdrawals; • Transactions via unrelated third parties.
Objectives	• Limited to domestic activities; • Clear mission statement corresponding the non-profit principles; • Limited to supplying goods or services.	• Lack of clarity on the purpose and nature of the NPO; • Inconsistency between the purpose and actual activities.
Industry Association	• Member of sector association; • Adherence to self-regulation standards; • ANBI status; • CBF seal.	• No sector association membership; • No applicable self-regulation standards.

Commensurate to these risk factors, and potentially in order to be able to identify the above risk factors, obliged entities will be required to cover the following elements in their risk assessments, without necessarily implying that EDD is in order:

a The customer's governance, including identifying who its beneficial owners, trustees and other persons with influence over the NPO are;

b How the NPO is funded, i.e. where its funds originate: private donations, government funds, etc., and how its funds are used;

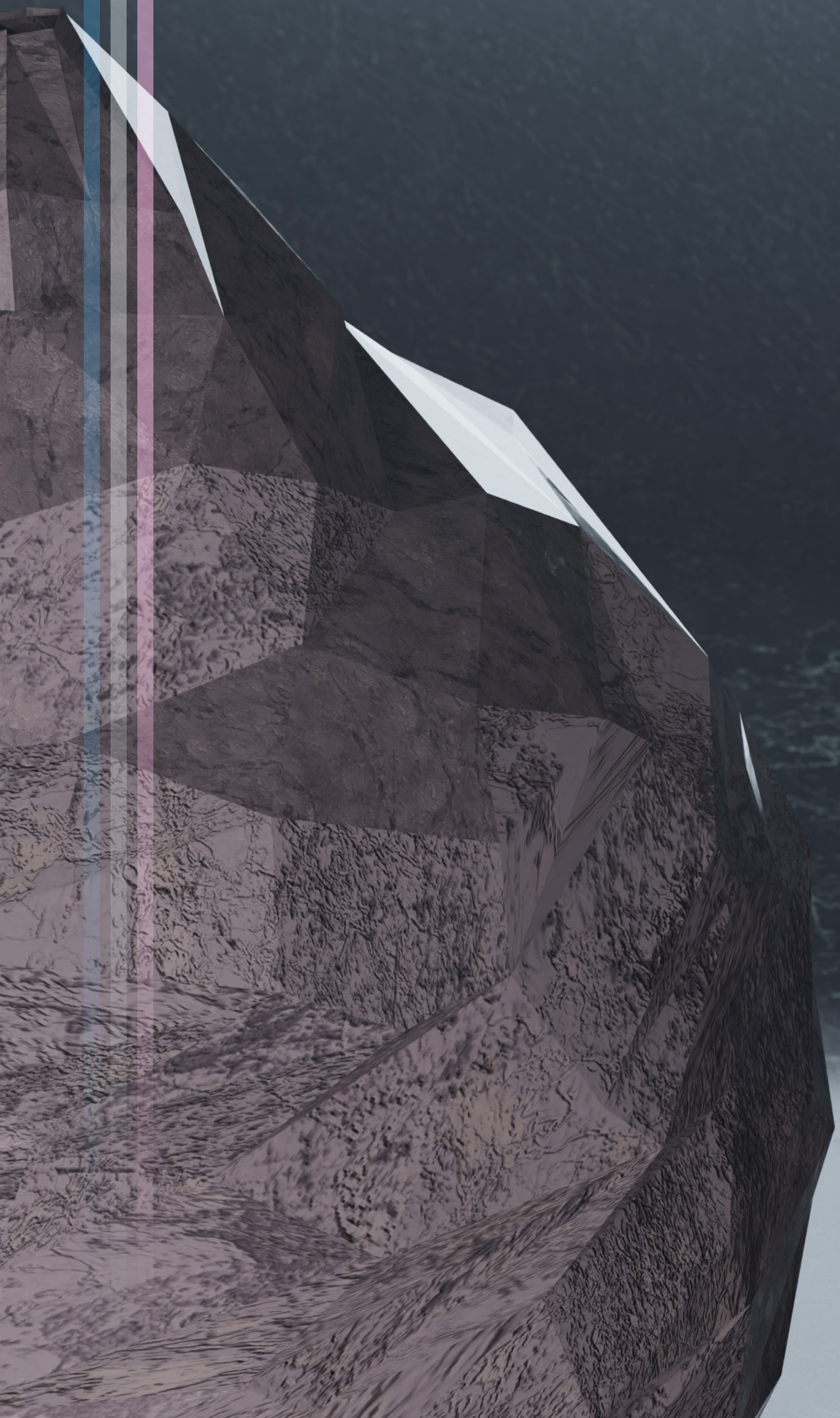
c What the objectives of the customer's operations are, which can be determined through the mission statement and the extent of actual objective performance of the operations;

d Which categories of beneficiaries benefit from the customer's activities, for example, refugees, legal entities that receive assistance through the services of the NPO or similar and how many beneficiaries there are;

e What transactions the NPO is likely to request, based on its objectives and activity profile, including payment of staff or providers posted abroad, and the expected frequency, size, and geographical destination of such transactions, information that is required to craft an effective ETP anyways;

f Where the NPO conducts its programmes and/or operations, in particular whether the NPO conducts its activities only in the Netherlands or also abroad, particularly in HRTCs.

10. CRYPTO-ASSET SERVICE PROVIDERS



10 CRYPTO-ASSET SERVICE PROVIDERS

At the moment, one of the most talked about topics in the financial sector involves the regulation of the market for crypto-assets and CASPs, a term included in art. 3(1)(15) of the Markets in Crypto-Assets Regulation ('**MiCAR**').[94] Although the concept of a CASP regulated under MiCAR is relatively new, a form of authorisation for certain virtual asset service providers ('**VASPs**') has already been implemented in EU member states by means of the AMLD4. This authorisation regime, which is included in art. 23b to 23j Dutch AML Act, solely sees to VASPs that provide (a) custodial wallet services, and/or (b) service for the exchange between virtual assets and fiat currency.[95] Although the distinction between VASPs and CASPs is of relevance, the latest Industry Baseline issued by the NVB consistently uses the acronym CASP, whilst seemingly mostly dealing with VASPs.[96] Although the Transfer of Funds Regulation ('**TFR**')[97], which came into effect in June 2023, will change the (outdated) definition of VASP included in the AMLD4, and therefore require an amendment of the Dutch AML Act, to CASP pending the application of MiCAR. The difference being that VASPs are not subject to continuous supervision by DNB, as was recently confirmed by the Dutch court,[98] contrary to CASPs which will be subject to full prudential supervision upon application of MiCAR. It is our view that VASPs will, until 1 January 2025, generally be considered to present heightened AML/CTF risk compared to CASPs when MiCAR is effective, especially given the recent warnings of FATF in respect of crypto-assets.[99] From hereon, we will use the acronym CASP in line with the Industry Baseline, however taking the aforementioned differentiation in regard.

On the whole, the CASP Industry Baseline provides for highly practical and useful guidance on the risk-based CDD process to be undertaken by banks in respect of CASPs (i.e. not the clients of CASPs) in line with their own risk appetite.[100] Much like the NPO Industry Baseline discussed above, a pre-CDD risk assessment is forwarded on the basis whereof the risk profile of the individual CASP is to be identified, avoiding the general exclusion of CASPs based on their sector's reputation foregoing mechanical application of EDD.[101] As part of their risk assessment, banks are most likely expected to reach out to CASPs extensively. However, it should

[94] Art. 3(1)(15) MiCAR: '[CASP] means a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis, and that is allowed to provide crypto-asset services [...].'

[95] Respectively the obliged entities included in art. 1a(4)(l) and (m) Dutch AML Act.

[96] NVB, Crypto-Asset Service Providers Industry Baseline, (2023).

[97] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.

[98] Rotterdam District Court, 4 October 2023, Digital Currency Services e.a./DNB, ECLI:NL:RBROT:2023:9157.

[99] FATF, Virtual Assets: Targeted Update on Implementation of the FATF Standards, (2023), paragraph 63: 'In light of increasing TF and PF threats related to [crypto-assets], including the theft of VAs by DPRK, the private sector and particularly [CASPs] should ensure they have appropriate risk identification and mitigation measures [...].' We also point out the fragility of compliance with the applicable sanctions regulation, when the CASP being dealt with is not regulated by itself, as the financial institution is obliged to also screen the clients of the CASPs

[100] DNB Q&A and Good Practices, GP 4.7.

[101] As required for high-risk activities pursuant to art. 8(1) Dutch AML Act; The TFR charges the EBA with developing guidelines on the EDD measures that may need to be applied to CASPs presenting a high-risk, which could comprise important forthcoming guidance for all obliged entities.

be possible to keep such contact to a minimum by obtaining as much as possible information by means of desk research. Information that may be requested from the CASP can be (a) information on governance and organisational structure, (b) proof of DNB registration, (c) AML/CTF audit reports,[102] (d) geographical location of activities, (e) information on client portfolio, and (f) indications as to the expected transaction behaviour. The Industry Baseline further clarifies that this assessment should also cover a VASP's Foundation client monies, insofar one exists.[103] Based on the pre-CDD risk assessment it can be assessed by the bank to what extent certain risk indicators exist which may suggest a higher, lower or more regular risk exposure. It must be noted that the Industry Baseline does not use the phrase SDD anywhere in the document, thus suggesting that at a minimum CASPs should be subject to regular CDD, which in our view seems to align with the legislation.[104] We refer to the Industry Baseline for an overview of the risk indicators, however, the categorisation of indicators follows that of the NPOs and has been based on draft guidance issued by the EBA.[105] We note that the draft EBA guidance on which the Industry Standard seem to be partly based, identifies unregulated CASPs as probably presenting a high-risk, thus probably warranting the application of EDD prior to the MiCAR becoming applicable, and afterwards to non-regulated CASPs.[106]

The Industry Baseline further touches on the manner in which banks are to deal with their clients purchasing or selling crypto assets. Clients that purchase crypto assets at a CASP, and to whom CDD (and if necessary, a source of funds investigation has been applied), shall not be considered as high risk ab ipso. In our view this may not be the case in the event where the CASP that is receiving the funds is located in a HRTC or is known to be a CASP that services crypto assets with certain anonymising functions (e.g. privacy coins). When a client is receiving funds from a CASP, for instance after selling crypto-assets and converting them into fiat currency, the client should be held to provide information to the bank on the source of funds, not the CASP. The Industry Baseline does not provide AML/CTF guidance to CASPs themselves, however for that reference is made to draft Guideline 21 setting sector specific measures for CASPs under the ML/TF Risk Factors Guidelines.

[102] Which should be assessed on a qualitative basis, as might the AML/CTF policies themselves, where in any instance a mere request and receival of the documentation shall not suffice.

[103] EBA, Consultation paper on the Guidelines amending the ML/TF risk factors Guidelines, (2023), p. 19: 'Guideline 9.16 is amended as follows: '9.16 Where a bank's customer opens a 'pooled/ omnibus account' in order to administer funds or crypto assets that belong to the customer's own clients, the bank should apply full CDD measures, including treating the customer's clients as the beneficial owners of funds held in the pooled account and verifying their identities.'

[104] As affirmed by the TFR in Recital (8): '[crypto-assets'] global reach, the speed at which transactions can be carried out and the possible anonymity offered by their transfer make virtual assets particularly susceptible to criminal misuse, including in cross-border situations.'

[105] EBA, Consultation paper on the Guidelines amending the ML/TF risk factors Guidelines, (2023), particular (draft) Guideline 21.

[106] EBA, Consultation paper on the Guidelines amending the ML/TF risk factors Guidelines, (2023), paragraph 28; As also the Dutch legislator considered, TK 2018-2019, Kamerstukken 35245 Nr. 3, p. 6; see also FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, (2021).

The Industry Baseline is a concrete manifestation of best practices, inspired by the ML/TF Risk Factors Guidelines, giving the sector concrete processes and data points to use when dealing with CASPs. This guidance is all the more welcome given the fact that the DNB Q&A and Good Practices remain largely silent on CASPs or crypto-assets, where their impact is left implicit – contrary to the notion of the EBA that sui generis guidance is needed in respect of this sector. We therefore welcome the Industry Baseline, although providing more practical guidance than a novel risk-based approach, as some of the more ambitious Industry Baselines seek to do.

11. CONCLUDING REMARKS

11. CONCLUDING REMARKS

The Industry Baselines provide a very welcome practical approach to the AML/CTF framework as applicable in the Netherlands. The concrete examples included in the Industry Baselines will give additional guidance to banks and other obliged entities in addition to fostering mutual understanding as to why a bank might be requesting certain information. It can only be welcomed that the customer will be faced with less moments of contact or information requests, which will enhance the customer's user experience and quite possibly its right to privacy. Equally welcome is the operational relief the risk-based approach the Industry Baselines offer in the form of large-scale automisation. The fact that the Industry Baselines are endorsed by DNB gives the Industry Baselines a level of legitimacy and authority that could not have been reached if the Industry Baselines were a mere codification of the best practices as applied by Dutch banks ab ipso.

Nevertheless, it can be questioned to what extend the explanation of the risk-based approach given by the NVB is always fully compliant with currently applicable AML/CTF regulation. It will be highly interesting to see how the new DNB Q&A and Good Practices and the Industry Baselines will coexist and how the subtle differences between them will be dealt with. One needs to remember that the Industry Baselines and DNB Q&A and Good Practices are based on the exact same legal framework as the DNB Guidance.[107] Furthermore, with the impending arrival of the AMLR, many of the subjects covered by the Industry Baselines will become actually more strict, such as data actualisation requirements, instead of more relaxed and cannot be waived on local interpretations, as it concerns a European Regulation.

The NVB has announced it will publish more Industry Baselines in the not too distant future, including sector specific Industry Baselines for those customers that currently face categorical exclusion due to de-risking by the banking sector, of which the NPO has been the first to be addressed. It seems foreseeable that subjects such as identification and verification of customers, and not just their UBOs, simplified due diligence and sanctions screening will be among the subjects covered.

[107] DNB, From recovery to balance A look ahead to a more risk-based approach to preventing and combating money laundering and terrorist financing, (2022).

The main question will be, however, whether the EBA might launch an investigation into a possible breach of Union law by DNB vis-à-vis the AMLD4 in its endorsement of the NVB Industry Baselines and the production of the DNB Q&A and Good Practices, or whether the EBA subscribes to the more balanced approach and continues a similar more risk-based trend in its guidance on ML/TF risks.