AML, CTF & Sanctions Guidance

Published by the NVB

15 July 2019

Nederlandse Vereniging van Banken

Content

Preface

These guidelines have been developed by the Dutch Bankers Association (Nederlandse Vereniging van Bank, hereinafter NVB) to set out risk factors that banks must consider when assessing the money laundering ("ML"), terrorist financing ("TF") and sanction risk associated with a customer relationship or occasional transaction. These guidelines also provide an outline how banks can adjust the extent of their customer due diligence ("CDD") measures in a way that is commensurate to the ML/ TF and/or sanction risk they have identified. The factors and measures described in these guidelines set out minimum requirements on the basis of the applicable regulatory framework and are not exhaustive. Banks must consider other factors and measures as appropriate.

Given the widespread use of the Guidance of the Joint Money Laundering Steering Committee ("JMLSG"), the NVB made use of the set-up and text in the Guidance of the JMLSG when writing these guidelines. JMLSG consists of the leading UK Trade Associations in the Financial Services Industry. Its aim is to promote good practice in countering ML and to give practical assistance in interpreting the UK Money Laundering Regulations.

Regulatory framework

The guidelines are primarily based on Dutch legislation. The Netherlands has had a long-standing obligation to have effective procedures in place to detect and prevent ML/TF and sanction violations. These procedures fall primarily within the scope of the following legislation and guidance:

- Anti-Money Laundering and Counter-Terrorist Financing Act[1] ("Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)");
- The Sanctions Act 1977[2] ("Sanctiewet (Sw)");
- The Financial Supervision Act[3];
- The Trust Offices Supervision Act[4];
- Dutch Economic Offences Act[5];
- DNB Guidance on Anti-Money Laundering and Counter Terrorism Financing Act and Sanctions act;
- Ministry of Finance 2013 Guidance on Wwft and Sw 1977.

Furthermore, the NVB also took into account the following European or international legislation and Guidance papers:

- Directive (EU) 2015/849; [6]
- ESA Joint Guidelines under Articles 17 and 18(4) Directive (EU) 2015/849;

.....

[1] Wet ter voorkoming van witwassen en terrorismefinanciering (Wwft)

[2] Sanctiewet 1977 (Sw). The Dutch sanctions guidelines are based on the Sanctions Act 1977. This is a framework act. Its application is governed by sanctions measures imposed by the EU. The EU has laid down sanctions measures in regulations and these have direct effect in all EU countries

[3] Wet op het financieel toezicht (Wft)

[4] Wet toezicht trustkantoren (Wtt)

[5] Wet op de Economische Delicten (WED)

[6] Directive (EU) 2018/843 – Will be included when transposed into national law.

- Wire Transfer Regulation on information accompanying transfers of funds (Regulation (EU) 2015/847);
- ESA Joint Guidelines under Article 25 of Wire Transfer Regulation;
- EU Sanctions Regulations;
- FATF 40 Recommendations;
- United Nations Security Council Resolutions;
- The Office of Foreign Assets Control ("OFAC");
- Basel Committee and its Core Principles;
- UK Joint Money Laundering Steering Committee ("JMLSG") and its recommendations.

Please note that Dutch banks are obliged to apply the legal provisions for the prevention of ML/TF violations in branches and majority-owned subsidiaries, insofar as the law of the jurisdiction concerned does not stand in the way of this. Should the law of the jurisdiction concerned prevent the application of the statutory regulations, the bank will notify the Dutch Central Bank ("DCB") and take measures to effectively manage the risk of ML/TF.

Purpose of this Guidance

The purpose of this Guidance is to:

- Outline the legal and regulatory framework for anti-money laundering (AML), countering terrorist financing (CTF) and sanction requirements and systems across the financial services sector;
- Interpret the requirements of the relevant law and regulations, and how they may be implemented in practice;
- Indicate good industry practice in AML/CTF procedures through a proportionate, risk-based approach; and
- Assist banks to design and implement the systems and controls necessary to mitigate the risks of the bank being used in connection with ML/, TF and sanction violations.

Scope of Guidance

The Guidance sets out what may be expected in relation to the prevention of ML, TF and sanction violations, but banks are ultimately responsible as to how they apply the requirements of the Dutch AML/CTF regime and sanction requirements in the particular circumstances of the bank, and its products, services, transactions and customers. By performing a Systematic Integrity Risk Assessment ("SIRA"), banks are expected to ensure sound and honourable business operations. The SIRA provides essential information about the activities of the different business operations and if applicable majority owned group entities. The outcome of the SIRA will constitute the basis for the AML/CTF control measures and must be reviewed regularly. This Guidance however does not deal with the specific requirements related to performing a SIRA.

The Guidance relates solely to how banks are expected to fulfil their obligations under the AML/ CTF and sanction law and regulations. The Guidance covers the prevention of ML/TF and sanction violations. ML/TF risks are closely related to the risks of other

financial crime, such as fraud and other predicate offences underlying ML and TF.[7] Predicate offences are not dealt with in the Guidance. The Guidance does, however, apply to dealing with any proceeds of crime that arise from these activities.

And finally, specific requirements in relation to systems and tooling for client filtering, transaction filtering and transaction monitoring falls outside the scope of these guidelines.

How should this Guidance be used?

Clearly, it is not the intention that the Guidance be applied unthinkingly, as a checklist of steps to take. Banks should encourage their staff to 'think risk' as they carry out their duties within the legal and regulatory framework governing AML/CTF. Banks must address their management of risk in a thoughtful and considerate way, and establish and maintain systems and procedures that are appropriate, and proportionate to the risks identified. This Guidance assists banks in doing this.

When provisions of the statutory requirements and of other regulatory requirements are referred to in the text of the Guidance, it uses the term must, indicating that these provisions are mandatory.

In other cases, the Guidance uses the term should to indicate ways in which the statutory and regulatory requirements may be satisfied, but allowing for alternative means of meeting the requirements. References to 'must' and 'should' in the text should therefore be construed accordingly.

The content of the Guidance

These guidelines are divided into two parts:

- Part I is general and applies to all banks. It is designed to equip banks with the tools they need to make informed, risk-based decisions when identifying, assessing and managing the ML/TF and sanction risk associated with individual customer relationships or occasional transactions.

- Part II is sector-specific and complements the general Guidance in Part I.[8] It sets out risk factors that are of particular importance in certain sectors and provides Guidance on the risk-sensitive application of CDD measures by banks in those sectors.

- These guidelines will help banks identify, assess and manage the ML/TF and sanction risk associated with individual customer relationships and occasional transactions in a risk-based, proportionate and effective way.

The NVB published a version of these guidelines to the NVB expertpool Wet en Regelgeving Criminaliteit for consultation. Respondents welcomed the draft guidelines

.....

[7] See for more guidance on the meaning of the concept of predicate offences the Interpretive note to recommendation 3 of FATF relating to the money laundering offence: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf .

[8] Part II will be published later this year

and responded that they would support the development of an effective risk-based approach to AML/ CFT and the prevention of sanction violations. Some respondents raised concerns. These concerns have been addressed in these guidelines as appropriate.

The NVB will keep these guidelines under review and update them as appropriate. These guidelines will be maintained by a working group reporting to the expert pool on statutory requirements relating to financial and economic crime[9] of the NVB. The NVB will confer on any changes made to the substance of these guidelines.

.....

[9] Expertpool Wet en Regelgeving Criminaliteit (EPWRC)

Chapter 1

Risk-based approach

1.1 Introduction and legal obligations

General

1.1.1 There are a number of discrete steps in assessing the most cost effective and proportionate way to manage and mitigate the ML, TF risks, proliferation financing risks, sanction risks, and tax risks faced by the bank. These steps are to:

- Identify the ML, TF, sanction and tax risks that are relevant to the bank;
- Assess the risks presented by:
  - the bank's particular customers and any underlying beneficial owners;
  - Products or services;
  - Transactions;
  - Delivery channels;
  - Geographical areas of operation;
- Design and implement controls to manage and mitigate these assessed risks, in the context of the bank's risk appetite;
- Monitor and improve the effective operation of these controls; and
- Record appropriately what has been done, and why.

In this chapter, references to 'customer' must be taken to include beneficial owner, where appropriate. A beneficial owner is usually an individual who ultimately owns or controls the customer or on whose behalf a transaction is being conducted.

Wwft 2a(1),3(1),(2)

1.1.2 Whatever approach is considered most appropriate to the bank's ML/TF risk, the broad objective is that the bank must know at the outset of the relationship who its customers (and, where relevant, beneficial owners) are, where they operate, what they do and their expected level of activity with the bank (e.g. requested products and services including if applicable a picture of the

expected transaction behaviour). The bank then must consider how the profile of the customer's financial behaviour builds up over time, thus allowing the bank to identify transactions or activity that may be suspicious.

1.2 Risk assessment

Wwft 2a, 2b(1), 2b(2), 3(1), (8), (9), 8, 9, 15, 16, Implementing decree Wwft 4 and Annex indicator list; Directive (EU) 2015/849, 6, 8, 11, 13, 16, 18, 20, 22, 23, 31, Annexes II and III; DNB Guidance on the AML/CTF and Sanctions Act 3.2, 3.3, 4.1.2, 4.1.5, 4.4, 4.5, 4,7 and 5.4; AFM Guidance on Wwft, Chapters 3, 5 and 7; Ministry of Finance Guidance Wwft, 2.2; FATF recommendations 10, 12, 15 and 17

1.2.1 The Wwft requires banks to take appropriate steps to identify and assess the risks of ML/TF to which its business is subject, taking into account:

- Information on ML/TF made available to them by the regulators;
- Risk factors, including factors relating to their customers, countries or geographic areas in which they operate, products, services, transactions and delivery channels.

When considering which steps are appropriate, banks must take into account the size and nature of its business. Banks that do not offer complex products or services and that have limited or no international exposure may not need an overly complex or sophisticated business risk assessment.

Obligation to adopt a risk-based approach

1.2.2 Senior management of most banks, whatever business they are in, monitor the bank's affairs with regard to the risks inherent to the business environment and jurisdictions the bank operates in, those risks inherent in its business and the effectiveness of the controls it has put in place to manage these risks.

1.2.3 To assist the overall objective to prevent ML/ TF, a risk-based approach:

- Recognises that the ML/TF threat to banks varies across customers, jurisdictions, products and delivery channels;
- Allows management to differentiate between their customers in a way that matches the risk in their particular business;
- Allows senior management to apply an approach that fits to the bank's resources, capabilities, procedures, systems and controls, and arrangements in particular circumstances and

- Helps to produce a sustainable effective system.

Wwft 3(8),(9); ESA Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849

1.2.4 A bank therefore uses its assessment of the risks inherent in its business to inform its risk-based approach to the identification and verification of each specific customer, which will in turn drive the level and extent of due diligence appropriate to that customer. The bank's decisions on the CDD measures to be applied must take account of Risk Factor Guidelines issued jointly by the European Supervisory Authorities.

1.2.5 No system of checks will detect and prevent all ML/TF. A risk-based approach will, however, serve to balance the cost burden placed on individual banks and their customers with a realistic assessment of the threat of the bank being used in connection with ML/TF. It focuses the effort where it is needed and will have most impact.

1.2.6 The appropriate approach in any given case is ultimately a question of judgement by senior management made in the context of the risks they determine the bank faces.

1.3 Risk assessment – identification and assessment of business risks

Decree on Prudential Rules for Financial Undertakings 10, Wwft 2c(1), Directive (EU) 2015/849 7

1.3.1 A bank is required to assess the risks inherent to its business, taking into account risk factors including those relating to its customers, countries or geographical areas in which it operates, products, services, its transactions and delivery channels; this is also known as Systemic Integrity Risk Analysis (SIRA). Risk management is in general a continuous process, carried out on a dynamic basis.

Wwft 2c(1), Directive (EU) 2015/849 7

1.3.2 The European Commission[10] as well as the Dutch government[11] publishes risk assessment reports on ML/TF which provides a backdrop to a bank's assessment of the risks inherent to its business. Banks must be aware of these publications and must take account of relevant findings that affect their individual

.....

[10] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing

[11] https://www.wodc.nl/onderzoeksdatabase/2689c-nra-witwassen-1.aspx / https://www.wodc.nl/onderzoeksdatabase/2689e-nra-terrorismefinanciering-1.aspx

business risk assessment. The Financial Action Task Force (FATF) publishes papers on the ML/TF risks in various industry sectors, see www.fatf-gafi.org.

Wwft 2b(3),(4), 3(11)

1.3.3 The risk assessments carried out must be documented, kept up to date and made available to the DNB on request. The DNB may decide that a documented risk assessment in the case of a particular bank is not required where the specific risks inherent to the sector in which the bank operates are clear and understood.

1.3.4 The risk environment faced by the bank includes the wider context within which the bank operates – whether in terms of the risks posed by the jurisdictions in which it and its customers operate, the relative attractiveness of the bank's products or the nature of the transactions undertaken. Risks are posed not only in relation to the extent to which the bank has, or has not, been able to carry out the appropriate level of CDD in relation to the customer or beneficial owner(s), nor by who the customer or its beneficial owner(s) is (are), but also in relation to the activities undertaken by the customer – whether in the normal course of its business, or through the products used and transactions undertaken. Banks should therefore assess its risks in the context of how it might most likely be involved in ML/TF. In this respect, senior management should ask themselves a number of questions; for example:

- What risk is posed by the bank's customers?
- What risk is posed by a customer's behaviour?
- How does the way the customer comes to the bank affect the risk?
- What risk is posed by the products/services the customer is using?

1.3.5 The business of many banks, their product and customer base, can be relatively simple, involving few products, with most customers falling into similar categories. In such circumstances, a simple approach, building on the risk the bank's products are assessed to present, may be appropriate for most customers, with the focus on those customers who fall outside the 'norm'. Other banks may have a wider range of business, but large numbers of their customers may be predominantly retail, served through delivery channels that offer the possibility of adopting a

standardised approach to many AML/CTF procedures. Here, too, the approach for most customers may be relatively straightforward, building on the product risk.

Wwft 2

1.3.6 For banks that operate internationally, or that have customers based or operating abroad, there are additional risk considerations related to the position of the jurisdictions involved, and their reputation and standing with respect to the inherent ML/TF risk, and the effectiveness of their AML/CTF enforcement regime.

1.3.7 Many governments and authorities carry out ML/TF risk assessments for their jurisdictions, and banks must take these into consideration, whenever they are published and available.

Delegated Regulation 2016/1675

1.3.8 The European Commission is empowered to identify high risk third countries with strategic deficiencies in the area of AML or CTF.[12]

Wwft 9, OECD, EC Country list

1.3.9 Countries may also be assessed using publicly available indices from FATF high-risk and non-cooperative jurisdictions[13], FATF evaluations, OECD and Transparency International Corruption Perceptions Index.

1.3.10 Annex 1-I includes further guidance on considerations banks might take account of in assessing the level of ML and TF risk in different jurisdictions.

Wwft 2c(1)

1.3.11 When the DNB issues a relevant thematic review report a bank must consider whether there are any areas of risk or issues of concern relevant to the bank's business that are highlighted within the report. Banks should be aware of the DNB's and AFM's published enforcement findings in relation to individual financial institutions, and their actions in response to these.

.....

[12] See http://eurlex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.L_.2016.254.01.0001.01.ENG. The Commission adopted Delegated Regulation 2016/1675 in July 2016.

[13] http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/

New technologies

Wwft 2a(2), ESA Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849, Title II, paras 10, 32, 33

1.3.12 In identifying and assessing ML/TF risks, banks must review whether new products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies for both new and pre- existing products. Apart from the specific requirement that it must be assessed whether there is a high risk of ML/TF in a particular situation, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. Appropriate measures should be taken to manage and mitigate those risks, including the application of enhanced due diligence measures where relevant in particular cases.

1.4 A risk-based approach – Design and implement controls

Wwft 2c(3), Decree on Prudential Rules for Financial Undertakings 14, 15, 16, 17

1.4.1 Once the bank has identified and assessed the risks it faces in respect of ML or TF – at EU level, national level and in relation to the bank itself - senior management must establish and maintain policies, controls and procedures to mitigate and manage effectively the risks of ML and TF identified in its risk assessment. These policies, controls and procedures must take into account the size and nature of the bank's business.

1.4.2 The policies, controls and procedures designed to mitigate assessed ML and/or TF risks should be appropriate and proportionate to these risks, and should be designed to provide an effective level of mitigation.

Wwft 2c(3),(4), 2d(1)

1.4.3 Banks must obtain approval from their senior management for the policies, controls and procedures that they put in place and for monitoring and enhancing any measures taken, where appropriate. In this context senior management is defined as those persons who determine the daily policy of a bank. If the day-to-day policy of a bank is determined by two or more persons, the bank shall designate one of these persons to be responsible for the bank complying with the provisions of the Wwft.

1.4.4 A risk-based approach requires the full commitment and support of senior management, and the active co-operation of business units. The risk-based approach needs to be part of the bank's philosophy and should as such be reflected in its procedures and controls. There needs to be a clear communication of policies, controls and procedures across the bank, along with robust mechanisms to ensure that they are carried out effectively, weaknesses are identified, and improvements are made wherever necessary.

Wwft 2c(1), 2d(2),(3),(4),3(1), (2), 16, 33, 35

1.4.5 The policies, controls and procedures referred to in paragraph 1.4.1 must include:

- Risk management practices, customer due diligence, reporting, record-keeping, training and awareness of staff, internal controls and compliance management;
- Where appropriate with regard to the size and nature of the business, an independent audit function to examine and evaluate the bank's policies, controls and procedures.

1.4.6 The nature and extent of AML/CTF controls will depend on a number of factors, including:

- The nature, scale and complexity of the bank's business;
- The diversity of the bank's operations, including geographical diversity;
- The bank's customer, product and activity profile;
- The distribution channels used;
- The volume and size of transactions;
- The extent to which the bank is dealing directly with the customer or is dealing through intermediaries, third parties, correspondents or non-face to face access;
- The degree to which the bank outsources the operation of any procedures to other (Group) entities.

Wwft 3(2)

1.4.7 The application of CDD measures is intended to enable a bank to form a reasonable belief that it knows the true identity of each customer and beneficial owner, and, with an appropriate degree of confidence, knows the types of business and transactions the customer is likely to undertake. The bank's procedures must include procedures to:

- Identify and verify the identity of each customer on a timely basis before offering products and services;
- Identifying the ultimate beneficial owner and taking reasonable measures to verify that person's identity so that the bank is satisfied that it knows who the ultimate beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;
- Assessing and, when appropriate, obtaining information on the purpose and intended nature of the customer relationship;
- Conducting ongoing monitoring of the customer relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the bank's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date;
- To establish whether the natural person representing the customer is authorized to do so and, if applicable, to identify the natural person and to verify his identity;

Take reasonable measures to verify whether the customer is acting on behalf of himself or on behalf of a third party.1.4.8. How a risk-based approach is implemented will depend on the bank's operational structure. For example, a bank that operates through multiple business units will need a different approach from one that operates as a single business. Equally, it will also be relevant whether the bank operates through branches or subsidiary undertakings; whether their business is principally face to face or non-face to face; whether the bank has a high staff/customer ratio and/or a changing customer base, or a small group of relationship managers and a relatively stable customer base; or whether their customer base is international (especially involving high net worth individuals) or largely domestic.

Wwft 2c(3)

1.4.9 Senior management must decide on the appropriate approach in the light of the bank's structure. The bank may adopt an approach that starts at the business area level, or one that starts from a lower level such as customer segments. Taking account of any geographical considerations relating to the customer, or the transaction, the bank may start with its customer assessments, and combine these assessments with the product and delivery channel risks; or it may choose an approach that starts with the

product risk, and then combine with the customer and delivery channel risks.

1.5 A risk-based approach – customer risk assessments

General

Wwft 2b

1.5.1 Based on the risk assessment that has been carried out, a bank will determine the level of CDD that must be applied in respect of each customer and beneficial owner. It is likely that there will be a standard level of CDD that will apply to the generality of customer, based on the bank's risk appetite.

ESA Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849

1.5.2 As regards ML and TF, managing and mitigating the risks will involve measures to verify the customer's identity; collecting additional information about the customer; and monitoring his transactions and activity, to determine whether there are reasons to assume that transactions may involve ML/TF. Part of the control framework will involve decisions as to whether verification may take place electronically, and the extent to which the bank can use customer verification procedures carried out by other financial institutions. Banks must determine the extent of their CDD measures on a risk-sensitive basis depending on the type of customer, customer relationship, product or transaction, distribution or channel risk. Annex 1-II includes a fuller list of illustrative risk factors a bank may address when considering the ML/TF risk posed by customer situations, consistent with Risk Factor Guidelines issued jointly by the European Supervisory Authorities, that banks must comply with.

1.5.3 To decide on the most appropriate and relevant controls for the bank, senior management must ask themselves which measures the bank must adopt, and to what extent, to manage and mitigate these threats/risks effectively, and in line with the bank's risk appetite. Examples of control procedures include:

- Introducing a customer identification programme that varies the procedures regarding customers appropriate to their assessed ML/TF risk;
- Requiring the quality of evidence – whether documentary, electronic or by way of third party assurance - to be of a certain standard;

- Obtaining additional customer information, where this is appropriate to their assessed ML/TF risk; and
- Monitoring customer transactions/activities.

It is possible to try to assess the extent to which each customer should be subject to each of these checks, but what is relevant is the balance of these procedures as appropriate to the risk assessed in the individual customer, or category of customer, to which he belongs.

1.5.4 A customer identification programme that is appropriate to reflect risk could involve:

- A standard information dataset to be held in respect of all customers;
- A standard verification requirement for all customers;
- More extensive due diligence (more identification checks and/or requiring additional information) on customer acceptance for higher risk customers;
- Where appropriate, more limited identity verification measures for specific lower risk customer/product combinations; and
- An approach to monitoring customer activities and transactions that reflects the risk assessed to be presented by the customer, which will identify those transactions or activities that may be unusual or suspicious.

Customer risk assessments

Wwft 2b

1.5.5 Although the ML/TF risks facing the bank fundamentally arise through its customers, the nature of their businesses and their activities, a bank must consider its customer risks in the context of the wider ML/TF environment inherent to the business and jurisdictions in which the bank and its customers operate. Banks should bear in mind that some jurisdictions have close links with other, perhaps higher risk, jurisdictions, and where appropriate and relevant this should be taken into account.

1.5.6 The risk posed by an individual customer may be assessed differently depending on whether the customer operates, or is based, in a jurisdiction with a reputation for ML/TF, or in one which has a reputation for strong AML/CTF enforcement. It can also be relevant whether, and to what extent, the customer has

contact or customer relationships with other parts of the bank, its business or the wider group to which the customer belongs.

1.5.7 In reaching an appropriate level of comfort as to whether the ML/TF risk posed by the customer is acceptable and can be managed, requesting more and more identification is not always the right answer - it is sometimes better to reach a full and documented understanding of what the customer does, and the transactions likely to be undertaken. Some businesses carry an inherently higher risk of being used for ML/TF purposes than others.

Wwft 5

1.5.8 If a bank can neither satisfy itself as to the identity of a customer or the beneficial owner, nor verify that identity, nor obtain sufficient information on the nature and intended purpose of the customer relationship, it must not enter into a new customer relationship and must terminate an existing one (see also 2.2.6).

Wwft 3(2)(d),4(1), Decree on Prudential Rules for Financial Undertakings 14(1)

1.5.9 While a risk assessment must always be performed at the inception of the customer relationship (although see paragraph 1.5.15 below), for some customers a comprehensive risk profile may only become evident once the customer has begun transacting through an account, making the monitoring of transactions and on-going reviews a fundamental component of a reasonably designed risk-based approach. A bank may also have to adjust its risk assessment of a particular customer based on information received from a competent authority.

1.5.10 Some other banks, however, often (but not exclusively) those dealing in wholesale markets, may offer a more ‘bespoke’ service to customers, many of whom are already subject to adjusted due diligence by lawyers and accountants for reasons other than AML/CTF. In such cases, the business of identifying the customer will be more complex but will take account of the considerable additional information that already exists in relation to the prospective customer.

General principles - use of risk categories and factors

Wwft 2b

1.5.11 In order to be able to implement a reasonable risk-based approach, banks must identify criteria to assess potential ML/TF risks. Identification of the ML/TF risks, to the extent that such

ML/TF risk can be identified, of customers or categories of customers, and transactions will allow banks to design and implement proportionate measures and controls to mitigate these risks.

ESA Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849

1.5.12 Annex 1-II includes a fuller list of illustrative risk factors a bank may address when considering the ML/TF risk posed by customer situations, consistent with Risk Factor Guidelines issued jointly by the European Supervisory Authorities, which banks must take into account.

Wwft 2b

1.5.13 When assessing the ML/TF risks relating to types of customers, jurisdictions or geographic areas, and particular products, services, transactions or delivery channel risks, a bank must take into account risk variables that are connected to those risk categories. These variables, either in themselves or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Examples of such variables include:

- The purpose of an account or relationship;
- The level of assets to be deposited by a customer or the size of transactions undertaken;
- The regularity or duration of the customer relationship.

ESA Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849, Ttile II, para 34

1.5.14 When assessing risks, banks must consider all relevant risk factors before determining what is the overall risk category and the appropriate level of mitigation to be applied.

1.5.15 A risk assessment will often result in a stylised categorisation of risk: e.g., high/medium/low. Criteria will be attached to each category to assist in allocating customers and products to risk categories, in order to determine the varied treatments of identification, verification, additional customer information and monitoring for each category, in a way that minimises complexity.

Weighting of risk factors

ESA Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849, Title II, paras 36, 37 and 38

1.5.16 When weighting risk factors, banks must make an informed judgement about the relevance of different risk factors in the context of a particular customer relationship or occasional

transaction. This often results in banks allocating different 'scores' to different factors – for example, banks may decide that a customer's personal links to a jurisdiction associated with higher ML/TF risk is less relevant in the light of the features of the product they seek. Consequently, banks have to define for themselves their risk-weighting position. Parameters set by law or regulation may limit a bank's discretion.

ESA Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849, para 37

1.5.17 Ultimately, the weight given to each of these factors is likely to vary from product to product and customer to customer (or category of customers) and from one bank to another. When weighting factors, banks should ensure that:

- Weighting is not unduly influenced by merely one factor,
- Economic or profit considerations do not influence the risk rating;
- Weighting does not lead to a situation where it is impossible for any business to be classified as high risk;
- Situations that national legislation or risk assessments identify as always presenting a high ML/TF risk cannot be over- ruled by the bank's weighting; and
- Banks are able to override any automatically generated risk scores where necessary. The rationale for the decision to override such scores must be documented appropriately.

ESA Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849, para 38

1.5.18 Where a bank uses automated systems, purchased from an external provider, to allocate overall risk scores in order to categorize customer relationships or occasional transactions, it must understand how such systems work and how it combines risk factors to achieve an overall risk score. A bank must always be able to satisfy itself that the scores allocated reflect the bank's understanding of ML/TF risk, and it should be able to demonstrate this to the DNB if necessary.

Wwft 2c(1)

1.5.19 When the DNB issues a relevant thematic review report, or updates its DNB Leidraad, as part of its ongoing assessment of ML/TF risks, a bank must consider whether there are any areas of risk or issues of concern which are relevant to the bank's business highlighted within the report.[14]

[14] See https://www.dnb.nl/nieuws/index.jsp

Risk assessment: Simplified CDD (SDD) also known as adjusted CDD

Directive (EU) 2015/849 13(1), Annex II non-exhaustive list of factors of potential lower risks, Wwft 3(1),6, 7
ESA guidance paper on risk factors paragraph 41 - 43

1.5.20 A bank's risk assessment must help it identify where it must focus its AML/CFT risk management efforts, both at customer on-boarding and for the duration of the customer relationship. As part of this, banks must apply the following CDD measures:

- Identifying the customer and verifying the customer's identity;
- Identifying the ultimate beneficial owner and taking reasonable measures to verify that person's identity so that the bank is satisfied that it knows who the ultimate beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;
- Assessing and, as appropriate, obtaining information on the purpose and intended nature of the customer relationship;
- Conducting ongoing monitoring of the customer relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the bank's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date;
- To establish whether the natural person representing the customer is authorized to do so and, if applicable, to identify the natural person and to verify his identity;
- Take reasonable measures to verify whether the customer is acting on behalf of himself or on behalf of a third party.

1.5.21 Banks may however determine the extent of these measures on a risk sensitive basis. CDD measures must help banks better understand the risk associated with individual customer relationships or occasional transactions. Banks must be able to demonstrate that the CDD measures they have applied are commensurate to the ML/TF risks identified.

1.5.22 Identifying a customer as carrying a higher risk of money laundering or terrorist financing does not automatically mean that he is a money launderer, or a financier of terrorism. Similarly, identifying a customer as carrying a lower risk of money laundering or terrorist financing does not mean that the customer

is not. Staff therefore need to be vigilant in using their experience and common sense in applying the bank's risk based criteria and rules.

1.5.23 Banks may apply Simplified Due Diligence (SDD), also known as adjusted CDD (hereafter referred to as SDD), in situations where the ML/TF risk associated with a customer relationship has been assessed as low. Banks must thereby consider the risk factos listed in annex II Directive (EU) 2015/849 This means that banks, before applying reduced CDD measures, must ascertain that the customer relationship presents a lower degree of risk.

1.5.24 Banks must not, however, judge the level of risk solely on the nature of the customer or the product. Before applying SDD, banks must demonstrate that the customer relationship is low risk further to a risk assessment on the customer. The information a bank obtains when applying SDD must enable the bank to be reasonably satisfied that its assessment that the risk associated with the relationship is low, is justified. It must also be sufficient to give the bank enough information about the nature of the customer relationship to identify any unusual or suspicious transactions.

ESA Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 para 45

1.5.25 SDD does not imply an exemption from any of the CDD measures. However, banks may adjust the amount, timing or type of each or all of the CDD measures in a way that is commensurate to the low risk they have identified. SDD measures banks may apply include but are not limited to:

- Adjusting the timing of CDD, for example where the product or transaction concerned has features that limit its use for ML/TF purposes, for example by:
    - Verifying the customer's or beneficial owner's identity during the establishment of the customer relationship or
    - Verifying the customer's or ultimate beneficial owner's identity once transactions exceed a defined threshold or once a reasonable time limit has lapsed. Banks must make sure that:
        (a) This does not result in a de facto exemption from CDD, that is, banks must ensure that the customer's or ultimate beneficial owner's identity will ultimately be verified;

(b) The threshold or time limit is set at a reasonably low level (although, with regard to TF, banks should note that a low threshold alone may not be enough to reduce risk);
(c) They have systems in place to detect when the threshold or time limit has been reached; and
(d) They do not defer CDD or delay obtaining relevant information about the customer where applicable legislation requires that this information be obtained at the outset;

- Adjusting the quantity of information obtained for identification, verification or monitoring purposes, for example by:
  - Verifying the identity on the basis of information, data or documentation obtained from one reliable and independent source only or
  - Assuming the nature and purpose of the customer relationship because the product is designed for one particular use only, such as leasing or savings products;
- Adjusting the quality or source of information obtained for identification, verification or monitoring purposes, for example by:
  - Accepting information obtained from the customer rather than an independent source when verifying the ultimate beneficial owner's identity (note that this is not permitted in relation to the verification of the customer's identity); or
  - Where the risk associated with all aspects of the relationship is very low, relying on the source of funds to meet some of the CDD requirements, for example where the funds are state benefit payments or where the funds have been transferred from an account in the customer's name at a member state bank;
- Adjusting the frequency of CDD updates and reviews of the customer relationship, for example carrying these out only when trigger events occur such as the customer looking to take out a new product or service with a higher ML/TF risk or when a certain transaction threshold is reached; banks must make sure that this does not result in a de facto exemption from keeping CDD information up-to-date;
- Adjusting the frequency and intensity of transaction monitoring.

The bank may (if permitted by local law or regulation) apply SDD measures. When assessing the ML/TF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, potentially lower risk situations may be influenced by:

- Customer risk factors;
- Country or geographic risk factors;
- Product, service, transaction or delivery channel risk factors.

1.5.26 Having a lower ML/TF risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

ESA Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 para 47

1.5.27 SDD does not exempt a bank from reporting unusual transactions to the FIU.

ESA Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 para 48

1.5.28 Where there are indications that the risk may not be low, for example where there are grounds to suspect that ML/TF is being attempted or where the bank has doubts about the veracity of the information obtained, SDD must not be applied. Equally, where specific high-risk scenarios apply and there is an obligation to conduct Enhanced CDD (EDD), SDD must not be applied.

Enhanced customer due diligence (EDD)

Annex III non-exhaustive list of factors of potential higher risks of Directive (EU) 2015/849

1.5.29 Banks must apply EDD measures in higher risk situations to manage and mitigate those higher risks appropriately. EDD measures cannot be substituted for regular CDD measures but must be applied in addition to regular CDD measures. EDD means additional scrutiny or specific measures focused on risk indicators that have been identified. Banks must assess identified risk indicators and if applicable apply EDD measures on the identified risk. Identified risks must not be seen in isolation but require a consolidated holistic approach and should be considered in the entirety of all available information on the customer. Seen in isolation, each risk may be acceptable, but the total sum of risks and their interrelation determines the risk

classification and may lead to unacceptable risk for the bank. See 1.5.48.
Areas of potentially higher risk are the following:

(1) Customer risk factors:

(a) The customer relationship is conducted in unusual circumstances;
(b) Customers that are resident in geographical areas of higher risk as set out in point (3);
(c) Legal persons or arrangements that are personal asset-holding vehicles;
(d) Companies that have nominee shareholders or shares in bearer form;
(e) Businesses that are cash-intensive;
(f) The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

(2) Product, service, transaction or delivery channel risk factors:

(a) Private banking;
(b) Products or transactions that might favor anonymity;
(c) Non-face-to-face customer relationships or transactions; without certain safeguards, such as electronic signatures;
(d) Payment received from unknown or unassociated third parties;
(e) New products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

(3) Geographical risk factors:

(a) Countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CTF systems;
(b) Countries identified by credible sources as having significant levels of corruption or other criminal activity;
(c) Countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;
(d) Countries providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

Wwft 8

1.5.30 Banks must apply EDD measures in case the customer relationship or transaction by its very nature carries a higher risk

of ML/TF. Depending on the risk banks may apply one or more of the following EDD measures in cases that appear to be high ML/TF risk:

- Adopt a lower UBO threshold;
- Obtain additional UBO verification documentation from a reliable and independent source, other than a self-declaration statement signed by an UBO, director or authorized representative;
- Identify all directors (excluding the non-executive directors).

1.5.31 Apart from the above, banks might need to take additional EDD measures for identification, verification or monitoring purposes. The EDD measures taken should be commensurate to the risks identified. For example, in certain high-risk situations it may be appropriate to increase the amount of information obtained for CDD purposes, while for other high risk situations it may be appropriate to focus on enhanced ongoing monitoring during the course of the customer relationship.

ESA Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 para 60

1.5.32 Banks will not need to apply all EDD measures listed below in all cases. For example, in certain high risk situations it may be appropriate to focus on enhanced ongoing monitoring in the course of the customer relationship. EDD measures banks may apply include:

- increasing the amount of information obtained for CDD purposes:
    i. Information about the customer's or beneficial owner's identity, or the customer's ownership and control structure, so as to be satisfied that the risk associated with the relationship is well known. This may include obtaining and assessing information about the customer's or beneficial owner's reputation and assessing any negative allegations against the customer or beneficial owner. Examples include:
        (a) Information about family members and close business partners;
        (b) Information about the customer's or beneficial owner's past and present business activities; and
        (c) Adverse media searches.
    ii. Information about the intended nature of the customer relationship, to ascertain that the nature and purpose of the customer relationship is

legitimate and to help banks obtain a more complete customer risk profile. It includes obtaining information on:

(a) The number, size and frequency of transactions that are likely to pass through the account so as to be able to spot deviations that may give rise to suspicions. In some cases, requesting evidence may be appropriate;

(b) Why the customer looks for a specific product or service, in particular when it is unclear why the customer's needs cannot be met better in another way, or in a different jurisdiction;

(c) The destination of funds; or

(d) The nature of the customer's or beneficial owner's business in order to better understand the likely nature of the customer relationship.

- Increasing the quality of information obtained for CDD purposes:

  i. Requiring the first payment to be carried out through an account verifiably in the customer´s name with a bank subject to CDD standards that are not less robust than those set out in Directive (EU) 2015/849; or

  ii. Establishing that the customer's source of funds used in the customer relationship and the source of wealth are not proceeds from criminal activity and are consistent with the bank's knowledge of the customer and the nature of the customer relationship. In those cases in which the risk associated with the relationship is particularly increased, verifying the source of funds and the source of wealth may be the only adequate risk mitigation tool. The sources of funds or wealth can be verified, among others, by reference to VAT and income tax returns, copies of audited accounts, pay slips, public deeds or independent and credible media reports.

- Increasing the frequency of reviews, in order to be satisfied that the bank can continue to manage the risk associated with the individual customer relationship or conclude that it no

longer corresponds to its risk appetite and to help identify any transactions that require further review, for instance by:

i. Increasing the frequency of reviews of the customer relationship, to ascertain whether the customer's risk profile has changed and whether the risk remains manageable;
ii. Obtaining the approval of senior management to commence or continue the customer relationship so as to ensure that senior management are aware of the risk their bank is exposed to and can take an informed decision about the extent to which they are equipped to manage that risk;
iii. Reviewing the customer relationship on a more regular basis to ensure any changes to the customer's risk profile are identified, assessed and, where necessary, acted upon; or
iv. Conducting more frequent or in depth transaction monitoring to identify any unusual or unexpected transactions that may give rise to suspicion of ML or TF. This may include establishing the destination of funds or ascertaining the reason for certain transactions.

Wwft 8(5), (6), (7), (8), (9), (11)

1.5.33 Banks must always apply specific EDD measures in the following cases:

- Where the customer, or the customer's ultimate beneficial owner, is a Politically Exposed Person (PEP). In case of life insurance and other investment-related insurance policies, the verification of the identity of the beneficiaries shall take place at the time of the payout. A bank must take reasonable measures to determine whether the beneficiary or the ultimate beneficial owner of the beneficiary of a life insurance policy is a PEP;
- Where a bank enters into a correspondent relationship with a respondent institution from a non-EEA state;
- Where a bank deals with a customer that resides or is established or has its seat in a country that has been designated by the European Commission as a state with higher risk of ML/TF;

- All complex and unusually large transactions, or unusual patterns of transactions, that have no obvious economic or lawful purpose.

Politically Exposed Persons

Wwft 8(5)

1.5.34 Banks that have identified that a customer or a beneficial owner is a PEP must always:

- Take adequate measures to establish the source of funds to be used in the customer relationship and the source of wealth in order to allow the bank to satisfy itself that it does not handle the proceeds from corruption or other criminal activity. The measures banks must take to establish the PEP's source of funds and the source of wealth will depend on the degree of high risk associated with the customer relationship. Banks must verify the source of funds and the source of wealth on the basis of reliable and independent data, documents or information where the risk associated with the PEP relationship is particularly high (refer to Annex 1-III for guidance for a risk based EDD on PEPs);
- Obtain senior management approval for entering into, or continuing, a customer relationship with a PEP. The appropriate level of seniority for sign-off must be determined by the level of increased risk associated with the customer relationship, and the senior manager approving a PEP customer relationship must have sufficient seniority and oversight to take informed decisions on issues that directly impact the bank's risk profile.

1.5.35 When considering whether to approve a PEP relationship, senior management should base their decision on the level of ML/TF risk the bank would be exposed to if it entered into that customer relationship and how well equipped the bank is to manage that risk effectively.

Wwft 8(5)(b)(3)

Banks must apply enhanced ongoing monitoring of both transactions and the risk associated with the customer relationship. Banks should identify unusual transactions and regularly review the information they hold to ensure that any new or emerging information that could affect the risk assessment is identified in a timely fashion. The frequency of ongoing monitoring must be determined by the level of high risk associated with the relationship.

Wwft 8(7) and (8)

1.5.36 Banks must apply all of these measures to PEPs, their family members and known close associates and should adjust the extent of these measures on a risk-sensitive basis. If the customer or the beneficial owner no longer holds a prominent public function, the bank shall apply appropriate risk-based measures for as long as necessary, but at least for 12 months, until that person no longer carries the higher risk associated with a politically prominent person.

Correspondent relationships

Wwft 8(4)

1.5.37 Banks must take specific EDD measures where they have correspondent relationships. Banks must apply all of these measures and must adjust the extent of these measures on a risk sensitive basis.

High risk jurisdiction designated by the European Commission

Wwft 9

1.5.38 When dealing with individuals or entities residing or established in a high risk third country identified by the Commission, and in all other high risk situations, banks should take an informed decision which EDD measures are appropriate for each high risk situation. The appropriate type of EDD, including the extent of additional information sought, and of the increased monitoring carried out, will depend on the reason why a relationship was classified as high risk.

Complex and unusually large transactions or unusual patterns

Wwt 8(3)

1.5.39 Banks must put in place adequate policies and procedures to detect unusual transactions or patterns of transactions. Where a bank detects transactions that are unusual because:

- They are larger than what the bank would normally expect based on its knowledge of the customer, the customer relationship or the category to which the customer belongs; or
- They have an unusual or unexpected pattern compared to the customer's normal activity or the pattern of transactions associated with similar customers, products or services; or

- They are very complex compared to other, similar transactions by similar customer types, products or services,

and the bank is not aware of an economic rationale or lawful purpose or doubts the veracity of the information it has been given, it must apply EDD measures

1.5.40 These EDD measures should be allow to help the bank to sufficiently and adequately determine whether these transactions give rise to suspicion and must at least include:

- Taking reasonable measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or finding out more about the customer's business to ascertain the likelihood of the customer making such transactions; and
- Monitoring the customer relationship and subsequent transactions more frequently and with greater attention to detail. A bank may decide to monitor individual transactions where this is commensurate with the risk it has identified.

Other considerations

ESA Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 para 60

1.5.41 As part of EDD banks should consider applying (manual) screening for adverse media attention.

1.5.42 Based on their risk appetite, the size of their customer base and its segmentation, their services or distribution channels used, banks may consider to perform adverse media screening for standard CDD purposes:

- As part of their customer onboarding process for certain customer segments;
- As part of their periodic review;
- As part of updating customer information;
- For all customers on an ongoing basis using a real time automated solution.

Wwft 5(3)

1.5.43 Banks must not enter into a customer relationship if they are unable to comply with their CDD requirements, if they are not satisfied that the purpose and nature of the customer relationship are legitimate or if they are not satisfied that they can effectively manage the risk that they may be used for ML/TF purposes. If

such a customer relationship already exists, banks should terminate it or suspend transactions until it can be terminated, subject to instructions from law enforcement, where applicable.

1.5.44 If some situations are assessed as high risk, or which are outside the bank's risk appetite, the bank may wish not to take on the customer, or may wish to terminate the relationship. This may be the case in relation to particular types of customer, or in relation to customers from, or transactions to or through, particular high risk countries or geographic areas, or in relation to a combination of other risk factors.

1.5.45 Although jurisdictions may be subject to economic sanctions, there may be some situations where for humanitarian or other reasons a bank may, under license, take on or continue with the customer or the business or transaction in, to, or through such high risk jurisdictions.

.

Wwft 16

1.5.46 Where based on the above considerations banks have reasonable grounds to suspect that ML/TF is being attempted, banks must report this to their FIU.

1.5.47 Banks should note that the application of a risk-based approach does not of itself require them to refuse, or terminate, customer relationships with entire categories of customers that they associate with higher ML/TF risk, as the risk associated with individual customer relationships will vary, even within one category.

Wwft 2b(1), 3(2)

1.5.48 The bank must decide, on the basis of its assessment of the risks posed by different customer/product combinations, on the level of verification that should be applied at each level of risk presented by the customer. Consideration should be given to all the information a bank gathers about a customer, as part of the normal business and vetting processes. Consideration of the overall information held may alter the risk profile of the customer.

Annex 1-I Considerations in assessing the level of ML/TF risk in different jurisdictions

1. This annex is designed to assist banks by setting out how they might approach their assessment of other jurisdictions, to determine their level of ML/TF risk. The Annex discusses jurisdictions where there may be a presumption of low risk, and those where such a presumption may not be appropriate without further investigation. It then discusses issues that a bank should consider in all cases when coming to a judgment on the level of ML/TF risk implicit in any particular jurisdiction.

Implications of an assessment as low risk

2. Assessment of a jurisdiction as low risk only allows for some easement of the level of due diligence carried out – it is not a complete exemption from the application of CDD measures in respect of customer identification. It does not exempt the bank from carrying out ongoing monitoring of the customer relationship with the customer.

3. It is therefore important that the reasons for concluding that a particular jurisdiction is low risk (other than those in respect of which a presumption of low risk may be made) are documented at the time the decision is made, and that it is made on relevant and up to date data or information.

Categories of country

(a) EU/EEA member states

4. When identifying lower risk jurisdictions, FATF encourages banks to take into consideration country risk factors:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems;
- Countries identified by credible sources as having a low level of corruption or other criminal activity.

In making a risk assessment, countries or banks could, when appropriate, also take into account possible variations in ML and TF risk between different regions or areas within a country.

5. All Member States of the EU are required to enforce legislation and financial sector procedures in accordance with the Directive (EU) 2015/849. The directive implements the revised 2012 FATF standards.

   All EEA countries have undertaken to implement the Directive (EU) 2015/849 and all are members of FATF or the relevant FATF style regional body (for Europe, this is MONEYVAL).

6. Given the commitment to implement the Directive (EU) 2015/849, banks may initially presume EEA member states to be low risk; significant variations may however exist in the precise measures that have been taken to transpose the ML directive (and its predecessors) into national laws and regulations. Moreover, the effective implementation of the standards will also vary. Whenever banks have substantive information indicating that a presumption of low risk cannot be sustained, either in general or for particular products, they will need to consider whether their procedures should be enhanced to take this information into account.

(b) FATF and FATF style regional body members

7. All FATF members, including members of FATF style regional bodies, undertake to implement the FATF AML and CTF Recommendations as part of their membership obligations.

8. However, unlike the transposition of the ML directive by EU Member States, implementation cannot be mandatory, and all members will approach their obligations in different ways, and follow different timetables.

9. Information on the effectiveness of implementation in these jurisdictions may be obtained through scrutiny of Mutual Evaluation reports, which are published on the FATF website, as well as through the FATF public statements and newsletters from DNB. Whenever banks have substantive information indicating that a presumption of low risk cannot be sustained, either in general or for particular products, they will need to consider whether their procedures should be enhanced to take this information into account.

(c) OECD members

10. The OECD promotes policies that improve the economic and social well-being of peole around the world. All members of the OECD are committed to implement the Recommendations of the Council. These Recommendations are a.o. about: responsible business conduct, good corporate governance, (public) integrity, combatting corruption and tax transparency.

11. The performance of the individual members is monitored by using a peer review process. The outcomes of these peer reviews are published on the OECD website and can provide insight in the effectiveness of the implemented Recommendations. Whenever banks have substantive information indicating that a presumption of low risk cannot be sustained, either in general or for particular products, they will need to consider whether their procedures should be enhanced to take this information into account.

(d) Other jurisdictions

12. A majority of countries and territories are not included in the lists of countries that can be presumed to be low risk This does not necessarily mean that the AML/CTF legislation, and standards of due diligence, in those countries are lower than those in other jurisdictions assessed as low risk. However, standards vary significantly, and banks will need to carry out their own assessment of particular countries. In addition to a bank's own knowledge and experience of the country concerned, particular attention should be paid to any FATF-style or IMF/World Bank evaluations that have been undertaken.

13. This is why, as a result of due diligence carried out for the purpose of determining those jurisdictions which, in the bank's judgement, are low risk, banks may rely as far as CDD measures are concerned on other regulated banks situated in such a jurisdiction.

Factors to be consider when assessing other jurisdictions

14. Factors include:

- Geographical risk factors;
- Membership of groups that only admit those meeting a certain benchmark;
- Contextual factors – political stability; level of (endemic) corruption etc.;
- Evidence of relevant (public) criticism of a jurisdiction, including FATF advisory notices;
- Independent and public assessment of the jurisdiction's overall AML regime;
- Need for any assessment to be recent;
- Implementation standards (inc quality and effectiveness of supervision).

Geographical risk factors

15. Geographical risk factors include:

- Countries identified by the EU Commission as having strategic deficiencies in their national AML/CFT regimes that pose significant threats to the financial system of the Union ('high-risk third countries) based on article 9 of Directive (EU) 2015/849;

- Countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter ML or TF;
- Countries identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism, ML , and the production and supply of illicit drugs;
- Countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
- Countries providing funding or support for terrorism;
- Countries that have organisations operating within their territory which have been designated by other countries, international organisations or the European Union as terrorist organisations.

Banks should bear in mind that the presence of one or more risk factors may not always indicate that there is a high risk of ML/TF in a particular situation.

Membership of an international or regional 'group'

16. There are a number of international and regional 'groups' of jurisdictions that admit to membership only those jurisdictions that have demonstrated a commitment to fight against ML/TF and which have an appropriate legal and regulatory regime to back up this commitment.

Contextual factors

17. Factors such as the political stability of a jurisdiction, and where it ranks in tables of corruption are relevant to whether it is likely that a jurisdiction will be low risk. It will, however, seldom be easy for banks to make their own assessments of such matters, and it is likely that they will have to rely on external agencies for such evidence – whether prepared for general consumption, or specifically for the bank. Where the bank looks to publicly available evidence, it will be important that it has some knowledge of the criteria that were used in making the assessment; the bank cannot rely solely on the fact that such a list has been independently prepared, even if by a respected third party agency.

Evidence of relevant (public) criticism

18. From time to time the FATF issues statements on its concerns about the lack of comprehensive AML/CTF systems in a number of jurisdictions (see section 2.4 below). When constructing their internal procedures, therefore, financial sector banks should look into the need for additional monitoring procedures for transactions from any country that is listed on these statements of concern. It will also be required to have additional monitoring procedures with respect to correspondent relationships with financial institutions from such countries.

19. Furthermore, other, commercial agencies also produce reports and lists of jurisdictions, entities and individuals that are involved, or that are alleged to be involved, in activities that cast doubt on their integrity in the AML/CTF area. Such reports lists can provide some useful and relevant evidence – which may or may not be conclusive – on whether or not a particular jurisdiction is likely to be low risk.

Mutual evaluation reports

20. Particular attention should be paid to assessments that have been made by standard setting bodies such as FATF, and by international financial institutions such as the IMF.

FATF

21. FATF member countries monitor their own progress in the fight against ML/TF through regular mutual evaluation by their peers. In 1998, FATF extended the concept of mutual evaluation beyond its own membership through its endorsement of FATF- style mutual evaluation programmes of a number of regional groups, which include non-FATF members. The groups undertaking FATF-style mutual evaluations are:

- The Offshore Group of Banking Supervisors (OGBS) see www.ogbs.net;
- The Caribbean Financial Action Task Force (CFATF) see www.cfatf.org;
- The Asia/Pacific Group on Money Laundering (APG) see www.apgml.org;
- MONEYVAL, covering the Council of Europe countries that are not members of FATF see www.coe.int/Moneyval;
- The Financial Action Task Force on Money Laundering in South America (GAFISUD) see www.gafisud.org;
- The Middle East and North Africa Financial Action Task Force (MENAFATF) see www.menafatf.org;
- The Eurasian Group (EAG) see www.eurasiangroup.org;
- The Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) see www.esaamlg.org;
- The Intergovernmental Action Group against Money-Laundering in Africa (GIABA) see www.giabasn.org.

22. Banks should bear in mind that mutual evaluation reports are drawn up at a 'point in time', and should be interpreted as such. Although follow up actions are usually reviewed after two years, there can be quite long intervals between evaluation reports in respect of a particular jurisdiction. Even at the point an evaluation is made there can be changes in train to the jurisdiction's AML/CTF regime, but these will not be reflected in the evaluation report. There can also be subsequent changes to the regime (whether to respond to criticism by the evaluators or

otherwise), which banks should seek to understand and to factor into their assessment of whether the jurisdiction is low risk.

23. In assessing the conclusions of a mutual evaluation report, banks may find it difficult to give appropriate weighting to findings and conclusions in respect of the jurisdiction's compliance with particular Recommendations. For the purpose of assessing the level of risk, compliance (or otherwise) with certain Recommendations may have more relevance than others. The extent to which a jurisdiction complies with the following Recommendations may be particularly relevant:

Legal framework:
Recommendations 1, 3, 4 and 5
Measures to be taken by banks:
Recommendations 9, 10, 11, 17 and 20,
Supervisory regime:
Recommendations 26, 27 and 35
International co-operation:
Recommendations 2 and 40

24. Summaries of FATF and FATF-style evaluations are published in FATF Annual Reports and can be accessed at www.fatf-gafi.org. However, mutual evaluation reports prepared by some FATF- style regional bodies may not be fully carried out to FATF standards, and banks should bear this in mind if a decision on whether a jurisdiction is low risk is based on such reports.

IMF/World bank

25. As part of their financial stability assessments of countries and territories, the IMF and the World Bank have agreed with FATF on a detailed methodology for assessing compliance with AML/CTF standards, using the FATF Recommendations as that basis. A number of countries have already undergone IMF/World Bank assessments in addition to those carried out by FATF, and some of the results can be accessed at www.imf.org. Where IMF/World Bank assessments relate to FATF members, the assessments are formally adopted by the FATF and appear on the FATF website.

Implementation standards (including effectiveness of supervision)

26. Information about the extent and quality of supervision of AML/CTF standards may be obtained from the manner in which a jurisdiction complies with Recommendations 17, 23, 29 and 30.

Advisory notices

FATF

27. The FATF issues periodic announcements about its concerns regarding the lack of comprehensive AML/CTF systems in various jurisdictions.

28. The FATF maintains a Public Statement that lists jurisdictions of concern in three categories:
    1. Jurisdictions subject to a FATF call on its members and other jurisdictions to apply countermeasures to protect the international financial system from ongoing and substantial ML/TF risks emanating from the jurisdiction.

    2. Jurisdictions with strategic AML/CTF deficiencies that have not committed to an action plan developed with the FATF to address key deficiencies. The FATF calls on its members to consider the risks arising from the deficiencies associated with each jurisdiction, as described below.

    3. Jurisdictions previously publicly identified by the FATF as having strategic AML/CTF deficiencies, which remain to be addressed.

29. The FATF also maintains a statement Improving Global AML/CTF Compliance: On-going Process, which lists jurisdictions identified as having strategic AML/CTF deficiencies for which they have developed an action plan with the FATF. While the situations differ among jurisdictions, each jurisdiction has provided a written high-level political commitment to address the identified deficiencies. The FATF will closely monitor the implementation of these action plans and encourages its members to consider the information set out in the statement.

DNB/ECB

30. DNB/ECB expects banks to keep abreast of revisions of the FATF Statements and to consider the impact of these statements when assessing jurisdictions.

Factors to be taken into account when assessing non transparant jurisdictions

31. The following factors may be taken into account when assessing non-transparent jurisdictions:

    a. The country is identified by the IMF as an Offshore Financial Centre: https://www.imf.org/external/NP/ofca/OFCA.aspx;

    b. The country is identified by the OECD as a jurisdiction committed to improving transparency and establishing an effective exchange of information in tax matters: http://www.oecd.org/countries/caymanislands/jurisdictions-

committed-to-improving-transparency-and-establishing-effective-exchange-of-information-in-tax-matters.htm.

c. The country is identified by the EU as a third country jurisdiction for tax purposes: https://ec.europa.eu/taxation_customs/tax-common-eu-list_en.

d. The country is identified by the Ministry of Finance: https://www.rijksoverheid.nl/actueel/nieuws/2018/12/28/nederland-stelt-zelf-lijst-laagbelastende-landen-vast-in-strijd-tegen-belastingontwijking;

e. Other countries might be added based on the banks' internal analysis.

Annex 1-II Illustrative risk factors relating to customer situations

I. Customer Risk Factors

A. Business or professional activity

Risk factors that may be relevant when considering the risk associated with a customer's or their beneficial owner's business or professional activity include:

- Does the customer or beneficial owner have links to sectors that are associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, arms trade and defence, extractive industries and public procurement?

- Does the customer or beneficial owner have links to sectors and/or industries that are associated with higher ML or TF risk, for example certain Money Service Businesses, gambling, dealers in precious metals, dealers in luxury goods, commercial real estate, virtual currencies platforms and e-wallet providers?

- Does the customer or beneficial owner have links to sectors that involve significant amounts of cash?

- Where the customer is a legal person, what is the purpose of their establishment? For example, what is the nature of their business?

- Does the customer have political connections, for example, are they a Politically Exposed Person (PEP), or is their beneficial owner a PEP? In what jurisdiction is the PEP, his business or a business he is connected with, located?

- Does the customer or beneficial owner hold another public position that might enable them to abuse public office for private gain? For example, are they senior or regional public figures with the ability to influence the awarding of contracts, decision-making members of high profile sports bodies or individuals that are known to influence the government and other senior decision-makers?

- Is the customer a legal person subject to enforceable disclosure requirements that ensure that reliable information about the customer's beneficial owner is publicly available, for example public companies listed on stock exchanges that make such a disclosure a condition for listing?

- Is the customer a credit or financial institution from a jurisdiction with an effective AML/CTF regime and is it supervised for compliance with local AML/CTF obligations? Is there evidence that the customer has been subject to supervisory sanctions or enforcement for failure to comply with AML/CTF obligations or wider conduct

requirements in recent years?

- Is the customer a public administration or enterprise from a jurisdiction with low levels of corruption?

- Is the customer's or their beneficial owner's background consistent with what the bank knows about their former, current or planned business activity, their business' turnover, the source of funds and the customer's or beneficial owner's source of wealth (if applicable)?

B. Reputation

The following risk factors may be relevant when considering the risk associated with a customer's or their beneficial owners' reputation:

- Are there any adverse media reports or other relevant information sources about the customer? For example, are there any allegations of criminality or terrorism in relation to the customer or their beneficial owners? If so, are these credible? Banks should determine the credibility of allegations on the basis of the quality and independence of the source data and the persistence of reporting of these allegations, among others. The absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing.

- Has the customer, beneficial owner or anyone publicly known to be closely associated with them had their assets frozen due to administrative or criminal proceedings or allegations of terrorism or TF? Does the bank have reasonable grounds to suspect that the customer or beneficial owner or anyone publicly known to be associated with them has, at some point in the past, been subject to such an asset freeze?

- Does the bank know if the customer or beneficial owner has been subject to a suspicious activity report in the past?

- Does the bank have any in-house information about the customer's or their beneficial owner's integrity, obtained, for example, in the course of a long-standing customer relationship?

C. Nature and behaviour

- The risk factors listed below may be relevant when considering the risk associated with a customer's or their beneficial owners' nature and behaviour (not all of these risk factors will be apparent at the outset, but may emerge only once a customer relationship has been established).

- Does the customer have legitimate reasons for being unable to provide robust evidence of his identity, perhaps because he is an asylum seeker?

- Does the bank have any doubts about the veracity or accuracy of the customer's or beneficial owner's identity?

- Are there indications that the customer might seek to avoid the establishment of a customer relationship? For example, does the customer intend to carry out one or several one-off transactions where the establishment of a customer relationship might make more economic sense?

- Is the customer a shell company? For example, it has no physical presence (other than a mailing address) and it generates little or no independent economic value.

- Is the customer incorporated in a non-transparent jurisdiction or are there entities in the ownership and control structure that are incorporated in non-transparent jurisdictions?

- Is the customer's ownership and control structure transparent and does it make sense? For example, are there many layers of intermediate parents or are there trusts or other complex entity types in the structure? If the customer's ownership and control structure is complex or opaque, is there an obvious commercial or lawful rationale?

- Does the customer issue bearer shares or have nominee shareholders?

- Does the customer make use of nominee directors or does it have multiple layers of legal entities as company directors?

- Is the customer a legal person or structure that could be used as an asset holding vehicle?

- Is there a sound reason for changes in the customer's ownership and control structure?

- Does the customer request transactions that are complex, unusually or unexpectedly large or have an unusual or unexpected pattern without apparent economic or lawful purpose or a sound commercial rationale? Are there grounds to suspect that the customer is trying to evade certain thresholds?

- Does the customer request unnecessary or unreasonable levels of secrecy? For example, is the customer reluctant to share CDD information, or do they appear to disguise the true nature of their business?

- Can the customer's or beneficial owner's source of wealth or source of funds be easily explained, for example by their occupation, inheritance or investments?

- Does the customer use their products and services as expected when the customer relationship was first established?

- Where the customer is a non-resident, could their needs be better serviced elsewhere? Is there a sound economic or lawful rationale for the customer requesting the type of financial service sought? Note that EU law creates a right for private individual consumers who are legally resident in the EU and have a real interest in The Netherlands to obtain a basic bank account, but this right applies only in sofar as

banks can comply with their AML/CTF obligations.

- Is the customer a non-profit organisation whose activities expose it to particularly high risks of abuse for TF purposes?

II. Countries and Geographic Areas Factors

When identifying the risk associated with countries and geographic areas, banks should consider the risk related to:

(a) The jurisdiction in which the customer or beneficial owner is resident/registered;
(b) The jurisdictions which are the customer´s or beneficial owner's main place of business; and
(c) The jurisdiction to which the customer or beneficial owner has relevant links.

Annex 2-I sets out further Guidance on considerations banks might take account of when assessing the level of ML/TF risk in different jurisdictions.

III. Products, Services and Transactions Risk Factors

When identifying the risk associated with their products, services or transactions, banks should consider the risk related to:

(a) The level of transparency, or opacity, afforded by the product, service or transaction;
(b) The complexity of the product, service or transaction; and
(c) The value or size of the product, service or transaction.

Risk factors that may be relevant when considering the risk associated with a product, service or transaction's transparency include:

- To what extent do products or services facilitate or allow anonymity or opacity of customer, ownership or beneficiary structures, for example pooled accounts, bearer shares, fiduciary deposits, offshore and certain trusts, or similar legal arrangements that are structured in a way to take advantage of anonymity and dealings with shell companies or companies with nominee shareholders that could be abused for illicit purposes?

- To what extent is it possible for a third party that is not part of the customer relationship to give instructions, e.g. certain correspondent banking relationships?

Risk factors that may be relevant when considering the risk associated with a product, service or transaction's complexity include:

- To what extent is the transaction complex and does it involve multiple parties or multiple jurisdictions, for example certain trade finance transactions? Are transactions straightforward, for example regular payments into a pension fund?

- To what extent do products or services allow payments from third parties or accept overpayments where this is not normally foreseen? Where third party payments are foreseen, does the bank know the third party's identity, for example a state benefit authority or a guarantor? Or are products and services funded exclusively by fund transfers from the customer's own account at another financial institution that is subject to AML/CTF standards and supervision that are comparable to those required under the regime of the Directive (EU) 2015/849?

- Does the bank understand the risks associated with its new or innovative product or service, in particular where this involves the use of new technologies or payment methods?

Risk factors that may be relevant when considering the risk associated with a product, service or transaction's value or size include:

- To what extent are products or services cash intensive, such as many payment services but also certain current accounts?

- To what extent do products or services facilitate or encourage high value transactions? Are there any caps on transaction values of levels of premium that could limit the use of the product or service for ML/TF purposes?

IV. Delivery Channel Risk Factors

When identifying the risk associated with the way the customer obtains the products or services they require, banks should consider the risk related to:

(a) The extent to which the customer relationship is conducted on a non-face to face basis; and
(b) Any introducers or intermediaries the bank might use and the nature of their relationship to the bank.

The bank may rely on certain third parties for the following CDD measures (see paragraph 5.6):

- Identifying the customer and verifying the customer's identity;
- Identifying, and where applicable, verifying the UBO's identity;
- Obtaining information on the purpose and intended nature of the customer relationship.

The responsibility for the CDD measures always remains with the bank. The bank must undertake its own risk assessment taking into account its specific relationship with the customer. Ongoing monitoring of the customer can only be carried out by the bank itself.

When assessing the risk associated with the way the customer obtains the product or services, banks should consider a number of factors including:

- Is the customer physically present for identification purposes? If they are not, has the bank used a reliable form of non-face to face CDD? Has it taken steps to prevent impersonation or identity fraud?

- Has the customer been introduced from other parts of the same financial group and if so, to what extent can the receiving unit of the group rely on this introduction as reassurance that the customer will not expose the receiving unit to excessive ML/TF risk? What has the receiving unit done to satisfy itself that the group entity applies CDD measures to NL standards?

- Has the customer been introduced by a third party, for example a bank that is not part of the same group, and is the third party a financial institution or is their main business activity unrelated to financial service provision? What has the bank done to be satisfied that:

    (I) The third party applies CDD measures and keeps records to NL standards and that it is supervised for compliance with comparable AML/CTF obligations in line with NL requirements?
    (II) The third party will provide, immediately upon request, relevant copies of identification and verification data, among others in line with NL requirements?
    (III) The quality of the third party's CDD measures is such that it can be relied upon?

- Has the customer been introduced through a tied agent, i.e. without direct bank contact? Has the agent obtained enough information so that the bank knows its customer and the level of risk associated with the customer relationship?

- If independent or tied agents are used, to what extent are they involved on an ongoing basis in the conduct of business? How does this affect the bank's knowledge of the customer and ongoing risk management?

Where a bank uses an intermediary, are they:

(I) A regulated person subject to AML obligations that are consistent with those of the NL regime?
(II) Subject to effective AML supervision? Are there any indications that the intermediary's level of compliance with applicable AML legislation or regulation is inadequate, for example because the intermediary has been sanctioned for breaches of AML/CTF obligations?
(III) Based in a jurisdiction associated with higher ML/TF risk? Where a third party is based in a high risk third country that the Commission has identified as having strategic deficiencies, banks must not rely on that

intermediary. However, reliance may be possible provided the intermediary is a branch or majority-owned subsidiary undertaking of another bank established in the EU, and the bank is confident that the intermediary fully complies with group wide policies, controls and procedures in line with NL requirements.

Annex 1-III Considerations in the treatment of politically exposed persons for anti-money laundering purposes

Banks apply a risk sensitive approach to identifying PEPs, being a customer or a UBO of a customer, and then apply enhanced due diligence measures. The legislation and guidance clarifies that a case-by-case basis is required with the risk assessment of individual PEPs rather than applying a generic approach to all PEPs.

Banks should identify when a PEP is a beneficial owner of a customer. It is not required that a legal entity should be treated as a PEP just because a PEP might be a beneficial owner.[15]

Once a bank is satisfied that a PEP is a beneficial owner then, in line with the risk-based approach, it assesses the risks posed by the involvement of that PEP and, after making this assessment, the bank applies appropriate measures. Banks may consider taking the guidance provided here into account. This could range from applying CDD measures in cases where the PEP is just a figurehead for an organisation (this will vary according to the circumstances of each entity but could be the case even if they sit on the board, including as a non-executive director) through to applying EDD measures, according to the risk assessed in line with this guidance where it is apparent the PEP has significant control or the ability to use their own funds in relation to the entity.[16]

When a PEP is a beneficial owner of a corporate customer, a bank may consider to not automatically treat other beneficial owners/shareholders of the customer as a PEP or known close associate, but may do so having assessed the relationship based on information available to the bank.[17]

Where customers do meet the definition of PEP because of the position they hold a bank may consider to recognise the lower risk of such customers and apply the guidance on

.....

[15] FCA Finalized Guidance 17/6: The treatment of politically exposed persons for anti-money laundering purposes, para 2.39

[16] FCA Finalized Guidance 17/6: The treatment of politically exposed persons for anti-money laundering purposes, para 2.40.

[17] FCA Finalized Guidance 17/6: The treatment of politically exposed persons for anti-money laundering purposes, para 2.41.

measures they can take in lower risk situations to meet their EDD obligations.[18] For example, obtaining approval from senior management[19] for establishing customer relationships does not need to imply, in all cases, obtaining approval from the board of directors or the echelon below. It should be possible for such approval to be granted by someone with sufficient knowledge of the bank's ML/ TF risk exposure and of sufficient seniority to take decisions affecting its risk exposure.[20]

Banks apply a more stringent approach where the customer is assessed as having a higher risk. In those circumstances banks will need to take further steps to verify information about the customer and the proposed business relationship. This is in line with the regulatory guidance to date where the focus has been on managing higher risk PEP relationships. This is because international standards issued by the Financial Action Taskforce (FATF) recognise that a PEP may be in a position to abuse their public office for private gain and a PEP may use the financial system to launder proceeds of this abuse of office. As FATF says 'these requirements are preventive (not criminal) in nature, and should not be interpreted as stigmatising PEPs as such being involved in criminal activity'.[21]

The following indicators suggest a PEP poses a lower risk:[22]
Lower risk indicators – product:

- The customer is seeking access to a product the bank has assessed to pose a lower risk.

Lower risk indicators – geographical:

- A PEP who is entrusted with a prominent public function in the Netherlands should be treated as low risk, unless a bank has assessed that other risk factors not linked to their position as a PEP mean they pose a higher risk. The risk factors guidance produced by the European Supervisory Authorities set out factors that might point to potential higher risk.
- A PEP may also pose a lower risk if they are entrusted with a prominent public function by a country where information available to the bank shows that it has the following characteristics:
    - Associated with low levels of corruption;
    - Political stability, and free and fair elections;
    - Strong state institutions;

.....

[18] FCA Finalized Guidance 17/6: The treatment of politically exposed persons for anti-money laundering purposes, paras 1.7 and 2.35.
[19] Senior management in relation to a customer or UBO as PEP is defined as:
a. persons who determine the day-to-day policy of a bank; or
b. persons working under the responsibility of a bank, holding a management position directly under the echelon of day-to-day policymakers and who are responsible for natural persons whose activities influence the exposure of a bank to the risks of ML and TF (see articles 1(1) and 8(5)(a)(1) Wwft).
[20] Directive 2015/849, preambule, para 34.
[21] www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf
[22] FCA Finalized Guidance 17/6: The treatment of politically exposed persons for anti-money laundering purposes, para 2.29

- Credible AML defences;
- A free press with a track record for probing official misconduct;
- An independent judiciary and a criminal justice system free from political interference;
- A track record for investigating political corruption and taking action against wrongdoers strong traditions of audit within the public sector;
- Legal protections for whistleblowers;
- Well-developed registries for ownership of land, companies and equities.

Lower risk indicators – personal and professional:
A PEP may pose a lower risk if they:

- Are subject to rigorous disclosures requirements (such as registers of interests, independent oversight of expenses);
- Does not have executive decision-making responsibilities (e.g. an opposition MP or an MP of the party in government but with no ministerial office).

Higher risk indicators – geographical:[23]

- A PEP may pose a greater risk if they are entrusted with a prominent public function in a country that is considered to have a higher risk of corruption. In coming to this conclusion, a bank should have regard to whether, based on information available, the country has the following characteristics;
- Associated with high levels of corruption;
- Political instability;
- Weak state institutions;
- Weak AML defences;
- Armed conflict;
- Non-democratic forms of government;
- Widespread organised criminality;
- A political economy dominated by a small number of people/entities with close links to the state;
- Lacking a free press and where legal or other measures constrain journalistic investigation;
- A criminal justice system vulnerable to political interference;
- Lacking expertise and skills related to book-keeping, accountancy and audit, particularly in the public sector;
- Law and culture antagonistic to the interests of whistleblowers;
- Weaknesses in the transparency of registries of ownership for companies, land and equities;
- Human rights abuses.

Higher risk indicators – personal and professional
The following characteristics might suggest a PEP is higher risk:

.....
[23] FCA Finalized Guidance 17/6: The treatment of politically exposed persons for anti-money laundering purposes, para 2.30

- Personal wealth or lifestyle inconsistent with known legitimate sources of income or wealth; if a country has laws that do not generally permit the holding of a foreign bank account, a bank should satisfy itself that the customer has authority to do so before opening an account;
- Credible allegations of financial misconduct (eg facilitated, made, or accepted bribes);
- Responsibility for, or able to influence, large public procurement exercises, particularly where procurement is not subject to competitive tender, or otherwise lacks transparency;
- Is responsible for, or able to influence, allocation of scarce government licenses such as mineral extraction concessions or permission for significant construction projects.

A family member or close associate of a politically exposed person may pose a lower risk if the PEP themselves poses a lower risk.[24] To clarify, banks may expect family or known close associates of NL PEPs to be treated as lower risk, unless there are circumstances to suggest otherwise.

The following characteristics might suggest a family member or close associates of a politically exposed person poses a higher risk:[25]

- Wealth derived from the granting of government licences (such as mineral extraction concessions, licence to act as a monopoly provider of services, or permission for significant construction projects);
- Wealth derived from preferential access to the privatisation of former state assets;
- Wealth derived from commerce in industry sectors associated with high-barriers to entry or a lack of competition, particularly where these barriers stem from law, regulation or other government policy;
- Wealth or lifestyle inconsistent with known legitimate sources of income or wealth;
- Credible allegations of financial misconduct (eg facilitated, made, or accepted bribes);
- Appointment to a public office that appears inconsistent with personal merit.

In lower risk situations a bank may take the following measures:[26]

- Seek to make no enquiries of a PEP's family or known close associates except those necessary to establish whether such a relationship does exist;

.....

[24] FCA Finalized Guidance 17/6: The treatment of politically exposed persons for anti-money laundering purposes, para 2.31

[25] FCA Finalized Guidance 17/6: The treatment of politically exposed persons for anti-money laundering purposes, para 2.32

[26] FCA Finalized Guidance 17/6: The treatment of politically exposed persons for anti-money laundering purposes, para 2.35

- Take less intrusive and less exhaustive steps to establish the source of wealth and source of funds of PEPs, family members or known close associates of a PEP; for example, only use information already available to the bank (such as transaction records or publicly available information) and do not make further inquiries of the individual unless anomalies arise. It is necessary to seek source of wealth information but in all lower risk cases, especially when dealing with products that carry a lower risk of laundering the proceeds of corruption, banks may consider to minimise the amount of information they collect and how they verify the information provided (for example, via information sources it has available);
- A customer relationship with a PEP or a PEP's family and close associates is subject to less frequent CDD review than if was considered high risk (for example, only where it is necessary to update CDD information or where the customer requests a new service or product).

In higher risk situations a bank may take the following measures:[27]

- Take more intrusive and exhaustive steps to establish the source of wealth and source of funds of PEPs, family members or known close associates of a PEP;
- A customer relationship with a PEP (or a PEP's family and close associates) is subject to more frequent and thorough formal review as to whether the customer relationship should be maintained.

.....

[27] FCA Finalized Guidance 17/6: The treatment of politically exposed persons for anti-money laundering purposes, para 2.36

Annex 1-IV Considerations in keeping risk assessments up to date

Banks should keep their assessment of ML/TF risk associated with individual customer relationships and occasional transactions, as well as the underlying factors, under review so as to ensure their assessment of ML/TF risk remains up to date and relevant. Banks should assess information obtained as part of their ongoing monitoring of the customer relationship and consider whether this affects the risk assessment.

Banks should also ensure that they have systems and controls in place to identify emerging ML/TF risks and that they can assess and, where appropriate, incorporate these in their business-wide and individual risk assessments in a timely manner.

Examples of systems and controls banks should put in place to identify emerging risks include:

- Processes to ensure internal information is reviewed on a regular basis to identify trends and emerging issues, both in relation to individual customer relationships and the bank's business;

- Processes to ensure the bank regularly reviews relevant information sources. This should involve, in particular:

    - Regularly reviewing media reports that are relevant to the sectors or jurisdictions the bank is active in;
    - Regularly reviewing law enforcement alerts and reports;
    - Ensuring that the bank becomes aware of changes to terror alerts and sanctions regimes as soon as they occur, for example by regularly reviewing terror alerts and looking for sanctions regime updates; and
    - Regularly reviewing thematic reports and similar publications issued by competent authorities.

- Processes to capture and reviewing information on risks relating to new products;

- Engagement with other industry representatives and competent authorities (such as round tables, conferences and training) and processes to feed back any findings to relevant staff; and

- Establishing a culture of information sharing within the bank and strong company ethics.

Examples of systems and controls banks should put in place to ensure their individual and business-wide risk assessment remains up to date include:

- Setting a date at which the next risk assessment update takes place, e.g. on the 1 March every year, to ensure new or emerging risks are included in the risk assessment. Where the bank is aware that a new risk has emerged, or an existing one has increased, this should be reflected in the risk assessment as soon as possible; and
- Carefully recording issues throughout the year that could have a bearing on the risk assessment, such as internal suspicious transaction reports, compliance failures and intelligence from front office staff.

Like the original risk assessments, any update of a risk assessment and adjustment of accompanying CDD measures should be proportionate and commensurate with the ML/TF risk.

Chapter 2

Customer due diligence

2.1 Meaning of customer due diligence measures and ongoing monitoring

2.1.1 This chapter gives guidance on the following:

The meaning of CDD measures: 2.1.4 – 2.1.13
Timing of and non-compliance with CDD measures: 2.2
Application of CDD measures: 2.3 – 2.5
Multipartite relationships, including reliance on third parties: 2.6
Identification and verification by third parties (outsourcing): 2.7
Monitoring customer activity: 2.8

Wwft 2b

2.1.2 Banks must determine the extent of their CDD measures and ongoing monitoring on a risk-sensitive basis, depending on the type of customer, customer relationship, product or transaction. They must be able to demonstrate to their supervisory authority that the extent of their CDD measures and monitoring is appropriate in view of the risks of ML/TF.

What is customer due diligence?

Wwft 3

2.1.3 The CDD measures that must be carried out involve:

(a) Identifying the customer, and verifying his;
(b) Identifying the beneficial owner, where relevant; verifying his identity;
(d) Assessing, and where appropriate obtaining information on, the purpose and intended nature of the customer relationship or transaction;Establishing whether the natural person representing the customer is authorized to do so and, if applicable, to identify the natural person and to verify his identity; and
(e) Taking reasonable measures to verify whether the customer is acting on behalf of himself or on behalf of a third party.

2.1.4 Where the customer is a legal person (other than a company listed on a Recognised Exchange), trust or similar legal

arrangement, banks must take reasonable measures to understand the ownership and control structure of that legal person, trust or similar legal arrangement.

2.1.5 Working out who is a beneficial owner may not be a straightforward matter. Different rules may apply to different forms of entity (refer to 2.5).

Wwft 6, 7, 8, 9

2.1.6 For some customer relationships, determined by the bank to present a low degree of risk of ML/TF, SDD (also knows as adjusted CDD) may be applied; in the case of higher risk situations, and specifically in relation to PEPs or correspondent relationships with non-EEA respondents, enhanced due diligence (EDD) measures must be applied on a risk sensitive basis.

For Guidance on applying SDD refer to 1.5.20 – 1.5.28.
For Guidance on applying EDD refer to1.5.29 – 1.5.48.

What is ongoing monitoring?

Wwft 3(2)(d), (11)

2.1.7 Bank's must conduct ongoing monitoring of the customer, including the scrutiny of transactions undertaken throughout the course of the relationship and keeping CDD information up to date. This is a separate, but related, obligation from the requirement to apply CDD measures.

Why is it necessary to apply CDD measures and conduct ongoing monitoring?

2.1.8 The CDD and monitoring obligations for banks under legislation and regulation are designed to make it more difficult for the financial services industry to be used for ML, TF or circumventing sanctions.

2.1.9 Banks also need to know who their customers are to guard against the risk of committing offences related to ML/,TF or circumventing sanctions.

2.1.10 Tax evasion is a predicate offence leading to ML. Failing to report knowledge or suspicions relating to such an activity is an offence committed by a bank.

2.1.11 This is why banks need to carry out customer due diligence and monitoring, for two broad reasons:

- To help the bank, at the time due diligence is carried out, to be reasonably satisfied that customers are who they say they are, to know whether they are acting on behalf of themselves, and that there is no legal barrier (e.g. government sanctions) to providing them with the product or service requested; and

- To enable the bank to report unusual transactions.

2.1.12 It may often be appropriate for the bank to know rather more about the customer than his identity: it will, for example, often need to be aware of the nature of the customer's business or activities in order to assess the extent to which his transactions and activity undertaken with or through the bank is consistent with that business.

2.2 Timing of, and non-compliance with, CDD measures

Wwft 3(5)

2.2.1 A bank must apply CDD measures when it does any of the following:

(a) Establishes a customer relationship;
(b) Carries out an occasional transaction;
(c) Suspects ML or TF; or
(d) Doubts the veracity of documents or information previously obtained for the purpose of identification or verification.

Timing of verification

Wwft 4(1),(2)

2.2.2 **General rule:** The verification of the identity of the customer and, where applicable, the beneficial owner, must, subject to the exceptions referred to below, take place before a customer relationship is established or a transaction is carried out.

2.2.3 **Exception if necessary, not to interrupt normal business and there is little risk:** Verification of the identity of the customer, and where there is one, the beneficial owner, may be completed during the establishment of a customer relationship if

(a) This is necessary so as not to interrupt the normal conduct of business; and
(b) There is little risk of the occurrence of ML/TF occurring

provided that verification is completed as soon as practicable after contact has been first established.

When this exception is applied for the opening of an account theverification of the identity of a customer (or beneficial owner, if applicable) may take place after the account (including an account which permits transactions in transferable securities) has been opened, provided that there are adequate safeguards in place to ensure that no transactions are carried out by or on behalf of the customer before verification has been completed.

2.2.4 **Other exceptions:** Where a bank is required to apply CDD measures in the case of a trust, a legal entity (other than a company) or a legal arrangement (other than a trust), and the beneficiaries of that trust, entity or arrangement are designated as a class, or by reference to particular characteristics, the bank must establish and verify the identity of the beneficiary before - any payment is made to the beneficiary, or the beneficiary exercises its vested rights in the trust, entity or legal arrangement.

Requirement to cease transactions, customer relationships etc.

Wwft 5(1), (3), 16(4)

2.2.5 Where a bank is unable to apply CDD measures in relation to a customer, the bank:

(a) Must not carry out a transaction through a bank account with or on behalf of the customer;
(b) Must not establish a customer relationship or carry out a transaction with the customer otherwise than through a bank account;
(c) Must terminate any existing customer relationship with the customer;
(d) Must consider whether it ought to be making a report to the FIU, in accordance with its obligations under the Wwft.

2.2.6 Banks must always consider whether an inability to apply CDD measures is caused by the customer not possessing the 'right' documents or information. In this case, the bank should consider whether there are any other ways of being reasonably satisfied as to the customer's identity. In either case, the bank must consider whether there are any circumstances constituting grounds for making a report to the FIU.

2.2.7 If the bank concludes that the circumstances do give reasonable grounds for knowledge of a suspicion of ML/TF, a report must be made to the FIU (refer to chapter 3).

2.2.8 If the bank concludes that there are no grounds for making a report, it will need to decide on the appropriate course of action.

Electronic transfer of funds

EC Regulation 2015/847

2.2.9 To implement FATF Recommendation 16, the EU adopted Regulation 2015/847, which came into force on 26 June 2017, and is directly applicable in all member states. The Regulation requires that payment services providers (PSPs) must include certain information in electronic funds transfers and ensure that the information is verified. The core requirement is that the payer's name, address and account number, and the name and payment account number of the payee, are included in the transfer, but there are a number of permitted exemptions, concessions and variations. Adequate CDD measures will support banks to meet these requirements.

2.2.10 The Regulation includes (among others) the following definitions:

- 'Payer' means a person that holds a payment account and allows a transfer of funds from that payment account, or where there is no payment account, that gives a transfer of funds order;
- 'Payee' means a person that is the intended recipient of the transfer of funds;
- 'Payment service provider' means a natural or legal person (as defined) providing transfer of funds services;
- 'Intermediary payment service provider' means a payment service provider that is not the payment service provider of the payer or of the payee and that receives and transmits a transfer of funds on behalf of the payment service provider of the payer or of the payee or of another intermediate payment service provider.

2.3 Application of CDD measures

Wwft 3(2)(a),(b),(c)

2.3.1 Applying CDD measures involves several steps. The bank is required to verify the identity of customers and, where applicable, beneficial owners. The purpose and intended nature of the customer relationship must also be assessed, and if appropriate, information on this obtained.

Identification and verification of the customer

DNB AML/Guidance 4.1.1

2.3.2 A “customer” is defined in the Wwft as a business, professional or commercial relationship between a bank and a customer, connected to the professional activities of the bank, and is expected by the bank at the time when contact is established to have an element of duration. The professional activities include the bank’s primary activities for which a licence was granted. However, if the bank offers certain activities that have a financial aspect with a risk of ML/TF, the bank will apply the Wwft to these activities. An example is transactions for telecom-companies (related to text or ‘0900’-services) that are provided by payment service providers. This means that relationships with professional counterparties in the context of the core activities of the bank, such as relationships with financial institutions and financial service providers, fall under the definition of correspondent relationships.
A relationship need not involve the bank in an actual transaction; giving advice may often constitute the start of a customer relationship.

Wwft 3(5)(b), (g) 2.3.3 An “occasional transaction” for CDD purposes means:

- A transfer of funds within the meaning of Regulation (EU) 2015/847 3(9) of the funds transfer regulation exceeding €1,000; or
- A transaction carried out other than in the course of a customer relationship (e.g., a single foreign currency transaction, or an isolated instruction to purchase shares), amounting to €15,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked.

2.3.4 The factors linking transactions to assess whether there is a customer relationship are inherent to the characteristics of the transactions – for example, where several payments are made to the same recipient from one or more sources over a short period of time, or where a customer regularly transfers funds to one or more sources. For lower-risk situations, which do not otherwise give rise to a customer relationship, a three-month period for linking transactions might be appropriate, assuming this is not a regular occurrence.

2.3.5 In general, the customer will be the party, or parties, with whom the customer relationship is established, or for whom the transaction is carried out. Where, however, there are several parties to a transaction, not all will necessarily be customers.

Wwft 3, 11, 33

2.3.6 The bank identifies the customer by obtaining a range of information about him. The verification of the identity consists of the bank verifying some of this information against documents, data or information obtained from a reliable source which is independent of the customer. Providing services to anonymous customers is not permitted.

2.3.7 For trusts or similar legal arrangements the following details are obtained and verified in addition:

- The purpose and nature of the trust or similar legal arrangement;
- The governing law by which the trust or similar legal arrangement is governed.

Developments in identification and verification

2.3.8 As a result of the technological innovation in the financial sector, new methods of (digital) verification of identity, specifically relating to online onboarding of customers, have been and are being developed, leading to remote identification and verification solutions. The application of remote (digital) verification of identity must be in line with applicable regulatory requirements. Given the inherent operational risks that new methods of digital verification present, its application also requires a risk assessment to identify, measure and manage potential risks.

The risk factors mentioned above are elaborated and concretised in the ESA's "Opinion on the use of innovative solutions by credit and financial institutions when complying with their customer due diligence (CDD) obligations."

Non-face to face business

Wwft 3, (8) (9)

2.3.9 A bank can take a risk based approach, meaning that the AML/CTF measures may vary in view of the specific risks the

bank has identified, but should be commensurate to those risks in order to mitigate them effectively. The nature and the extent of the CDD measures depends on the risks involved, including the type of customer, the nature of the relationship, the product or the transaction.
A bank shall at least take into account the risk factors referred to in Annex III to the Directive (EU) 2015/849, in order to determine whether that paragraph, applies.

Directive (EU) 2015/849 18(3) Annex III

2.3.10 The following is a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in Annex III Directive (EU) 2015/849 18(3), part (c) non-face to face customer relationships or transactions, without certain safeguards, such as electronic signatures.

ESA Guidelines section 32[28]

2.3.11 Delivery Channel Risk; to the extent to which the customer relationship is conducted on a non-face to face basis where no adequate additional safeguards – for example electronic signatures, electronic identification certificates issued in accordance with Regulation (EU) 910/2014[29] and anti-impersonation fraud checks – are in place. In such cases, identification and verification take place within the risk framework of a remote customer. In this event there is an increased risk and it is necessary to take additional measures to compensate for this risk. These obligations are based on article 13, second paragraph, of the Directive (EU) 2015/849 and FATF Recommendation 8. This is a clear example of a more principle-based approach. Prescribed is what result the due diligence should lead to, viz the proper verification of the identity of the customer. It is not prescribed how it should be carried out. In accordance with the Directive, the legislator chose to give some guidance by - not exhaustively - a number of possible measures[30].

.....

[28] https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf

[29] This Regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.

[30] Parliamentary Papers II 2007/08, 31 238, no. 6, p. 10 (NvW II). This also follows explicitly from the text of Article 13, second paragraph, of the Directive, which refers to 'for example'.

Enhanced due diligence measures

Wwft 8

2.3.12 The obligation to perform enhanced due diligence in case there is a higher risk of ML/TF does remain. Enhanced due diligence should primarily be performed if a customer relationship or transaction is by nature one that represents a higher risk. Banks must perform a risk assessment prior to entering into a customer relationship or executing a transaction, to determine whether there is a higher risk. To this end reference is made to the risk factors listed in Annex III to the Directive (EU) 2015/849 and which banks must in any case take into account in their risk assessment.

Wwft 8(2)(a), 11(1)

2.3.13 Article 8 (2) Wwft prescribes that measures must be taken to compensate for the higher risks as reflected in Annex III of Directive 2015/849. Under subsection 2 of this annex non face to face activities are included. The regulator has identified the following three types of measures:

- Verifying the identity of the client on the basis of additional documents, data and information that have been submitted
- Assesing the documents for authenticity; or
- Ensuring that the first payment related to the customer relationship or transaction holds, is credited or debited from a client's account – briefly said - a licensed financial institution in the EU / EEA the so-called 'derived identification', who may reasonably be assumed to have performed adequate CDD.

In addition, there are a number of other measures to consider and it cannot be ruled out that new possible (technical) measures will emerge in the “future” .

Directive (EU) 2015/849 18-24, ESA The Risk Factors Guidelines items 32 and 49

2.3.14 When identifying the risk associated with the way in which customers obtain the products or services they require, banks should consider the risk related to the extent to which the customer relationship is conducted on a non-face to face basis. When assessing the risk associated with the way in which the customer obtains the products or services, banks should consider a number of factors including:

- Has the bank used a reliable form of non-face to face CDD and has it taken steps to prevent impersonation or identity fraud?

- Banks must apply EDD measures in higher risk situations to manage and mitigate those risks appropriately. EDD measures cannot be substituted for regular CDD measures, but must be applied in addition to regular CDD measures.

Approach on controls and or additional measures

2.3.15 *Additional documents, data and information*
This means that with regard to the customer who is not physically present, further documents, data and information are required, in addition to the documents, data and information required for the verification of the identity of customers who are physically present. Verification of the identity of a customer, being a natural person, should be performed on the basis of documents, data and information from reliable sources independent of the customer.[31] These are in any case the well-known – also accepted identity documents already known under the Act on identification (Wet op de identificatieplicht, hereinafter Wid). For example a passport, Dutch identity card, an identity card issued by an EU Member State and a Dutch driving license. In any case, the additional documents, data and information must ultimately lead to the verification of the identity of the customer. It is self-evident that a document issued by a government agency or judicial authority is reliable. Depending on the risk assessment also other (additional) documents can be accepted, for example the following documents, data or information:

- Bank statement;
- A statement from an (independent) third party, such as a notary, an accountant, or another institution under (comparable) supervision at home or abroad;
- Gas and electricity bill;
- Salary slip;
- Labor contract;
- Public sources.

2.3.16 As far as a document is needed, an original or a copy can be requested. Of course, an original provides more certainty that the information is correct, but the requesting original documents are more difficult for both the bank and the customer. If the documents do not come from public authorities or judicial authorities, one may question whether the documents are sufficiently reliable. Such documents will in themselves often be

[31] Wwft 11

insufficient to adequately verify the identity, but they can serve as additional information. It goes without saying that documents from public authorities or from a regulated sector - in principle - can be regarded as relatively reliable. Documents from another source or documents that are easy to obtain without certainty that adequate identification and verification have preceded it, such as student cards, employee cards, (some) foreign driving licenses (without photo or from certain countries), are in themselves not sufficient to verify the identity.

2.3.17 *Assess authenticity document*

Banks have to assess the submitted documents for authenticity. This does not mean that if a bank chooses to compensate the higher risk by requesting additional documents, data and information (as described above), the authenticity of this information does not matter. In the end, it is all about that the identity of the client being established and verified. Ways to check the authenticity include but are not limited to:

- Checking internal external systems, such as EVA, SFH and VIS;
- Making use of external parties that can check the security features of identity documents;
- Verifying by means of the original identity document (to be returned by the bank);
- A statement or note on the document of an independent third party (see above) that the document is genuine;
- New technology on mobile identification with adequate safeguards.

2.3.18 *Derived identification*

In the case of derived identification, identification of the customer takes place by making use of the identification previously collected by another institution, a bank. With this form of identification, it is important that there is sufficient certainty that the client has identified himself elsewhere and that in this way he can be traced via a paper trail. This is why only the identification of banks in the other EU/EEA Member State can be used.

This form of identification means that the bank ensures that the first payment related to the customer relationship or the transaction is made in favor of or at the expense of an account of the customer with that bank. This bank will have established and verified the identity of the customer for the opening of this account on the basis of the Wwft or similar foreign legislation.

Banks can therefore assume that the customer's details are correct.

This method of identification was originally introduced to meet the technological developments that made it increasingly possible to provide financial services from a distance. The starting point for remote identification of customers was to meet both the requirement of flexibility, in particular with regard to the ability to adapt to technical developments, and to the requirement of security, to ensure adequate identification.

2.3.19 *Other measures*
The above mentioned measures follow from the law. This is a non-exhaustive list. Banks are therefore free to take other measures to identify and verify identity of a non-face to face customer. Finally banks will have to be comfortable that the measures are sufficiently adequate. A measure that is still mentioned, but that is not automatically included in one of the previous measures, is to establish independent contact with the customer.

Identification and verification of a beneficial owner

2.3.20 A beneficial owner is usually an individual who ultimately owns or controls the customer or on whose behalf a transaction is being conducted.

2.3.21 In respect of private individuals in general the customer him- or herself is the UBO, unless there are features of the transaction, or surrounding circumstances, that indicate otherwise. Therefore, there is no requirement for banks to make proactive searches for UBOs in such cases, but they should make appropriate enquiries where it appears that the customer is not acting on his/her own behalf. Where a customer, who is a private individual, is fronting for another individual who is the UBO, the bank must obtain the same information about that UBO as it would for a customer.

2.3.22 In case of a life insurance policy, if the UBO of the life insurance is not designated as a named person, but only on the basis of characteristics or as a category, then the bank obtains sufficient information regarding the UBO to be satisfied that at the time of payment the identity of the beneficiary can be established. Verification of the identity of the UBO takes place at the time of

payment of the life insurance policy. If a life insurance policy is transferred to the bank, the bank shall identify the UBO at the time of the transfer to the natural person, legal entity or legal arrangement that will receive the value of the transferred policy for their own benefit.

2.3.23 The UBO must always be identified and verified. Banks do not have a choice as to whether or not to verify the identity of the UBO depending on the risk involved: the bank must always take reasonable measures to verify his/her identity.

2.3.24 The *identification* of the UBO consists of obtaining the following details:

- Full name(s) (i.e. first name(s) and surname(s));
- Date of birth;
- Country of permanent residence;
- Size and nature of the beneficial owner (through ownership and/or control).

2.3.25 The *verification* of the UBO requirement consists of verifying:

- Full name(s) (i.e. first name(s) and surname(s));
- Date of birth;
- Capacity of the beneficial owner.

Directive (EU) 2015/849 28(2)(a),(b), (4)(b),(18), Wwft 3(2)(a)(b), 11

2.3.26 The verification requirements differ between a customer and a beneficial owner. The identity of a customer or beneficial owner must be verified on the basis of documents, data or information obtained from a reliable source that is independent of the customer. For these purposes, documents issued or made available by an official body are to be regarded as being independent of a person even if they are provided or made available to the bank by or on behalf of that person. The obligation to verify the identity of a beneficial owner, however, is for the bank to take reasonable measures so that it is satisfied that it knows who the beneficial owner is. It is up to each bank to consider whether it is appropriate, in the light of a ML/TF risk associated with the customer relationship, to make use of records of beneficial owners in the public domain, ask their customers for relevant data, require evidence of the beneficial owner's identity on the basis of documents, data or information obtained from a reliable source.

2.3.27 In general it may be reasonable for the bank to confirm the UBO's identity based on information supplied by the customer. This could include information provided by the customer (including trustees or other representatives whose identities have been verified) as to their identity, and confirmation that they are known to the customer. While this may be provided orally or in writing, any information received orally should be recorded in written form by the bank. If there are reasons to doubt the statement from the customer, the bank will take additional verification measures to establish the UBO.

2.3.28 In case of higher risk of misrepresentation, the use of a statement from the customer for example through the use of a self-declaration form is not sufficient and additional documentation and information from (other) reliable sources is required. One could think of, relevant additional data or documents from the customer and other sources.

2.3.29 It must be noted that banks may not exclusively rely on UBO-information registered by the customer in the public UBO-register. There may be situations where the bank based on its knowledge of the customer and its organisation structure or as a result of the relationship contacts and or contracts establishes that a natural person other than the one registered in the UBO-register actually exercises decive control over the customer. In those cases the bank must rely on its own observations and consider reporting this to the relevant authorities.

Existing customers

2.3.30 As risk dictates, therefore, banks must take steps to ensure that they possess appropriate information to demonstrate that they are satisfied that they know all their customers. Where the identity of an existing customer has already been verified to a previously applicable standard then, in the absence of circumstances indicating the contrary, the risk is likely to be low. A range of trigger events that may change the risk profile of the customer, such as an existing customer requesting for specific additional products or services or establishing a new relationship, might prompt a bank to seek appropriate evidence.

2.3.31 A bank may possess considerable information in respect of a customer of some years' standing. In some cases the issue may be more one of collating and assessing information already held

than approaching customers for more identification data or information.

Acquisition of one financial services firm, or a portfolio of customers, by another.

2.3.32 When a bank acquires the business and customers of another financial institution, either as a whole, or as a portfolio, it is not necessary for the identity of all existing customers to be re-verified, provided that:

- All underlying customer records are acquired with the business; or
- A warranty is given by the acquired financial institution, or by the vendor where a portfolio of customers or business has been acquired, that the identities of its customers were verified.

2.3.33 It is, however, important that the acquiring bank's due diligence enquiries include some sample testing in order to confirm that the customer identification procedures previously followed by the acquired financial institution (or by the vendor, in relation to a portfolio) have been carried out in accordance with Dutch AML/CFT requirements.

2.3.34 In the event that:

- The sample testing of the customer identification procedures previously undertaken shows that these have not been carried out to an appropriate standard; or
- The procedures cannot be checked; or
- The customer records are not accessible by the acquiring bank,

verification of identity will need to be undertaken as soon as is practicable for all transferred customers who are not existing verified customers of the transferee, in line with the acquiring bank's risk-based approach, and the requirements for existing customers opening new accounts.

Nature and purpose of proposed customer relationship

Wwft 3(2)(c)

2.3.35 A bank must understand the purpose and intended nature of the customer relationship or transaction to assess whether the proposed customer relationship is in line with the bank's

expectation and to provide the bank with a meaningful basis for ongoing monitoring. In some instances this will be self-evident, but in many cases the bank may have to obtain information in this respect. Usually, part of the required information is already obtained during contact with the customer prior to the establishment of a customer relationship. The purpose of the relationship will also be apparent from the services or products used by the customer. Additional queries from the bank can be aimed at obtaining clarification on the product user or service recipient. For customers not located or residing in the country where the bank is operating its services from (thus any country different than the customer owner location), the bank should establish as to why the customer intends to use its services or products from that location. If that is for tax purposes for example, the bank assesses the acceptability of that purpose.

2.3.36 By gathering this information the bank can assess any risks that may arise from the provision of services to the customer.

2.3.37 Depending on the bank's risk assessment of the situation, carried out in accordance with the guidance set out in Chapter 1, information that might be relevant may include some or all of the following:

- Nature and details of the business/occupation/employment;
- The purpose of an account or relationship;
- The anticipated level and nature of the activity that is to be undertaken through the relationship;
- The regularity or duration of the customer relationship;
- The level of assets to be deposited by a customer or the size of transactions undertaken.

2.3.38 Purpose and nature inquiries establish, to the extent applicable and required, as to what type of transactions the customer intends to perform (such as including number, frequency and size).

If the bank is not satisfied that the purpose and nature of the customer relationship is legitimate, the bank should not enter into a such relationship. For existing customers, where the same concern arises, a bank should consider terminating the relationship (subject to law enforcement where applicable).

2.3.39 Having a lower ML/TF risk for identification and verification purposes does not automatically mean that the same customer is

lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

2.3.40 When assessing the ML/TF risks related to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, banks should take into account risk variables related to those risk categories, including those set out in the ESA Risk Factor Guidelines[32] (see 1.5.20 – 1.5.48). These variables, either on their own or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Examples of such variables include:

- The purpose of an account or relationship,
- The level of assets to be deposited by a customer or the size of transactions undertaken;
- The regularity or duration of the customer relationship.

Source of funds and source of wealth

Legal requirements and industry standards

Wwft 3(2)(d), 9(2)(a)

2.3.41 Banks must continuously monitor the customer relationship and transactions carried out during the duration of this relationship in order to ensure that they correspond to the bank's knowledge of the customer and its risk profile. If necessary, banks are required to further examine the source of funds/assets used in the customer relationship or transaction.

Wwft) 3(2)(d)

2.3.42 A bank must establish, where needed, the source of the funds that will be used in the relationship or transaction on a risk-based approach. A bank must document this assessment. Where necessary, the bank must record statements and documentary evidence in customer files and ask further questions. In high-risk situations, especially, it is appropriate that the plausibility of the funds be determined and recorded using reliable sources (see annex 2-I for examples). To determine the plausibility that the funds will originate from a legitimate source, the bank must identify specific indicators that determine the depth of the review.

.....

[32] These Guidelines were published on 26 June 2017, to take effect by 26 June 2018. See https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%2 9.pdf

The bank can consider combinations of indicators, such as the amount involved, the reason given for the source of funds, business activities of the customer, country of origin or destination of the source of funds, and the provided product or service. In order to verify the source of the funds used in the customer relationship, it may also be necessary, especially with high-risk customers, to have an understanding of the customer's asset position. When customers spread their assets, the bank also needs to be aware of the other assets in order to be able to define a correct risk profile.

ESA Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849, Title II

2.3.43 A bank must monitor transactions to ensure that they are in line with the customer's risk profile and business and, where necessary, examine the source of funds, to detect possible ML/TF risk. Banks must satisfy themselves that they do not handle the proceeds from corruption or other criminal activities. The level of due diligence will depend on the degree of high risk associated with the customer relationship. Banks must note that these risk factors may emerge only once a customer relationship has been established. Risk factors include the following:

- The customer aims to carry out one transaction or several one-off transactions where the establishment of a customer relationship might make more economic sense;
- The customer requests transactions that are complex, unusually or unexpectedly large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or a sound commercial rationale;
- There are grounds to suspect that the customer is trying to evade specific thresholds such as those set out in Article 11(b) of Directive (EU) 2015/849 or in the appendix to Article 4 of the Wwft Implementation Decree 2018;
- The source of funds cannot easily be explained by the customer's activities.

Where the risk is particularly high and/or where the bank has doubts about the legitimate origin of the funds, verifying the source of funds may be the only adequate risk mitigating tool. The source of funds can be verified with reference to (non-exhaustive):

- An original or certified copy of contract of sale of, for example, investments or a company;
- Written confirmation of sale signed by a lawyer or solicitor;
- An internet search of a company registry to confirm the sale of a company.

Wwft 8(5)(b)(2)

2.3.44 Banks must take appropriate steps to determine the source of wealth in case a customer or ultimate beneficial owner is a PEP. In addition they must also take appropriate measures to establish the source of funds used in the transactions/business relationship for such a customer involving a PEP.

DNB Guidance on the AML/CTF and Sanctions Act 4.5

2.3.45 If the customer or ultimate beneficial owner becomes or proves to be a PEP in the course of the customer relationship, the bank must take additional measures as quickly as possible. Establishing the source of wealth of an ultimate beneficial owner who is a PEP can be difficult in some situations, although the intensity of the efforts to do so can be geared to the risk. In cases where it proves impossible to establish the source of wealth, the bank can demonstrate that it has made sufficient effort to establish the source of wealth.

ESA Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849, Title II

2.3.46 Banks that have identified that a customer or ultimate beneficial owner is a PEP must always take adequate measures to establish the source of funds to be used in the customer relationship and the source of wealth in order to allow the bank to satisfy itself that it does not handle the proceeds from corruption or other criminal activities. The measures banks must take to establish the PEP's source of funds and the source of wealth will depend on the degree of high risk associated with the customer relationship. Banks must verify the source of funds and wealth on the basis of reliable and independent data, documents or information where the risk associated with the PEP relationship is particularly high (see for more guidance Annex 1-III).

FCA Finalized Guidance 17/6: The treatment of politically exposed persons for anti-money laundering purposes, paras 1.7 and 2.35

2.3.47 Even if a customer does meet the definition of PEP because of the position they hold, a bank may decide to recognise the lower risk of such customers and apply the guidance on measures they can take in lower risk situations to meet their EDD obligations.

2.3.48 This means that in lower risk situations a bank may take less intrusive and less exhaustive steps to establish the source of funds and source of wealth of PEPs, family members or known close associates of a PEP; for example, only use information already available to the bank (such as transaction records or

publicly available information) and do not make further inquiries into the individual unless anomalies arise (for example by screening or transaction behaviour). In principle it is necessary to seek source of wealth information but in all lower risk cases, especially when dealing with products that carry a lower risk of laundering the proceeds of corruption, banks may consider minimising the amount of information they collect and how they verify the information provided (for example, via information sources it has available).

2.3.49 If the PEP has a UBO status as a consequence of being a senior managing official, banks may consider not to establish the source of wealth of the senior managing official when the source of funds of the customer does not stem from the source of wealth of the senior managing official. In such a case, the reason for not collecting further information on the source of wealth of a senior managing official should be clarified in the CDD file.

2.3.50 Similarly, in case of a lower risk situation a bank may decide not to make enquiries into a PEP's family or known close associates except those necessary to establish whether such a relationship does exist. This would entail that the source of wealth of family members or known close associates of a PEP may not be established when the PEP-position is held in a country assessed as being at a lower risk of large-scale corruption (because of the system and checks and balances in place that reduce the threat). In such a situation, banks may consider to only assess the source of wealth of those with true executive power and not their family members or known close associates.

Guidance regarding source of funds and source of wealth

2.3.51 *Source of funds and source of wealth defined*
The difference between source of funds and source of wealth can be explained as follows:

Source of funds: Means the origin of the funds involved in a customer relationship or occasional transaction. It includes both the activity that generated the funds used in the customer relationship, for example the customer's salary, as well as the means through which the customer's funds were transferred.

Source of wealth: Means the origin of the customer's or beneficiary's total wealth, for example an inheritance or savings.

2.3.52 The plausibility of the source of funds used in the customer relationship or transaction must be established. The bank must establish:

(1) That the customer's assets were plausibly introduced to the bank and that there is clarity on the funds passing through the customer's account and

(2) The plausibility of the source of funds/assets when entering into and monitoring a customer relationship and if necessary, verify the origin of the assets in a risk-based manner. The information provided should be credible (plausibility requirement). The intensity of the assessment performed should be geared to the risk identified.

Elements to be considered are:

- Whether the source of funds are in line with the overall customer profile (i.e. purpose and nature of the customer relationship);
- Whether the source of funds are plausible based on the statements of the customer;
- Whether the source of funds are plausible on the basis of other sources, such as public sources or transaction systems within the bank;
- Whether the assets are plausible given the business activities of the customer.

Other elements to consider are that:

- The description of the source of funds might be less detailed or might be difficult to verify on the basis of public sources, if the assets were entered into the bank account more than five years ago;
- The longer ago the assets were acquired, the sooner the bank can accept limited information;
- However, the bank must satisfy itself that the source of funds is legitimate. The bank must be wary of over-reliance on customer explanations; vague responses should be clarified and/or challenged.

2.3.53 In situations where there is doubt about the information provided or where there are certain red flags further due diligence may be required. The plausibility of the source of funds and/or assets should then be determined based on independent, reliable sources. The information/documentation provided should offer an answer to the question whether the bank can reasonably come to

the conclusion that the funds come from a legitimate source. In order to establish the plausibility of the source of funds involved in a customer relationship, it may be necessary in certain increased risk situations to have an understanding of the customer's asset position, for example in case of private banking clients.

Wwft 8(5)(b)(2)

2.3.54 In case a customer or ultimate beneficial owner is a PEP, not only appropriate measures to establish the source of funds must be taken, but also the source of wealth in order to allow the bank to satisfy itself that it does not handle the proceeds from corruption or other criminal activities.

Wwft 8(5)(b)(2)

2.3.55 The steps banks must take to establish the PEP's source of funds and the source of wealth will depend on the degree of high risk associated with the customer relationship. Banks should verify the source of funds and the source of wealth on the basis of reliable and independent documents, data and information where the risk associated with the PEP relationship is particularly high. The intensity of the efforts to do so can be adjusted to the risk. In cases where it proves impossible to establish the source of wealth, the bank must be able to demonstrate that it has made sufficient efforts to discover the source of wealth.

2.3.56 Banks can distinguish between a PEP as customer or PEP as UBO. If a UBO is identified as a PEP, the PEP must be assessed for his/her impact/influence on the customer and the intensity of the due diligence performed may be adjusted to the risk.

Elements to be considered are whether:

- The PEP has decision-making powers;
- The PEP is able to abuse his/her politically exposed position;
- The PEP has (in)direct control of or access to (governmental) funds;
- The PEP provides public services;
- The PEP, in its daily activities, has common interaction with the government concerning permits, tenders or checks.
- The UBO PEP is able to comingle personal assets with those of a corporate entity he/she owns.

ESA Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849, Title II

2.3.57 The level of due diligence must be established on the basis of a holistic view of the risk associated with a particular customer relationship or occasional transaction. Whether the source of

funds, and, where applicable, the source of wealth are plausible, must be assessed in the light of all other risk factors identified in relation to a particular customer relationship or occasional transaction. Thus a bank must perform enhanced due diligence in case a customer relationship or transaction by its nature or in relation to the country where the client resides or is established or has his seat poses a higher risk of ML/TF. Certain combinations of risk factors, may lead to enhanced due diligence, and if necessary, verification of the origin of the assets.

Refer to Annex 2-I for an overview of possible due diligence requirements regarding the source of wealth.

Keeping information up to date

Directive (EU) 2015/849 28(11)(b), Wwft 3(11)

2.3.58 Documents, data and information obtained for the purpose of applying CDD measures, held about customers, must be kept up to date. Once the identity of a customer has been verified, there is no obligation to re-verify identity (unless doubts arise as to the veracity or adequacy of the evidence previously obtained for the purpose of customer identification); as risk dictates, however, banks must take steps to ensure that they have appropriate up-to-date information on their customers. A range of trigger events, such as an existing customer requesting a specific additional product or service or establishing a new relationship, might prompt a bank to seek appropriate evidence.

2.4 Private individuals

Characteristics and evidence of identity

2.4.1 Paragraphs 2.3.2 to 2.3.8 refer to the standard identification requirement for customers who are private individuals. The paragraphs below provide further guidance on steps that may be applied as part of a risk-based approach. This paragraph describes how identification and verification of the private individuals takes place. For each customer it is first indicated whether identification and verification for the identity and/or role must take place. It is subsequently described how identification and verification of the identity and/or role could take place.

2.4.2 Identification and verification is a crucial step in the CDD proces, both with new and existing customers. It is important to establish with whom the bank does business directly or indirectly and to establish that the identity and role/authority stated in identification correspond with the actual identity and role of the statement of identity. The reason for this is that if the results are based on unverified data, it is not certain that the assessment has been done correctly. Under the Wwft it is mandatory to establish and verify the identity of customers and relevant related parties involved and to conduct the CDD proces on verified data.

2.4.3 CDD consists of identifying the customer and verifying his identity. A clear distinction must be made between identification and the verification of identity. For example, identification means that the bank of a customer/private individual obtains the first name(s), surname, address and date of birth either from the customer himself or from a third party (free of form). The concept of verification means establishing that these customer details are correct, based on reliable data, documentation and information from an independent source. The sources may vary using a risk-based approach.

Identification

Wwft 3(2)(a), 33(2)(a)

2.4.4 A bank must identify a new customer, so that the identity details of the customer become known. Providing services to an anonymous customer are therefore not allowed.

The bank must obtain and register the following information in relation to the private individual:

- Full name (given name(s) and surname(s));
- Date of birth;
- Residential address including country;
- Record the type, number, date and place/country of issue of the identification document with which the identity of the customer has been verified.

Verification

Wwft 11(1), 33(1), (2)(a)

2.4.5 Evidence of the identity must be based on information, data or documentation from a reliable source independent of the customer and can be obtained in various ways. In respect of natural persons, much weight is placed on so-called 'identity documents', such as a passport. For verification purposes the use of (certified copies of) identity documents is still prevailing.

2.4.6 It is however possible to have a reasonable belief as to a customer's identity based on several methods of verification. This can be different documents but also information and electronic/digital data held by various organisations. These documents, information and data vary in integrity, comprehensiveness, reliability and independence in terms of their technology and content. There is a broad range of possible sources (e.g., including but not limited to government departments, agencies, public sector bodies, local authorities, regulated financial institutions, and commercial organisations etc.). How much identity documentation, data and information is needed in order to have a reasonable belief as to a customer's identity can be assessed using a risk -based approach, taking into account all inherent ML/TF risk indicators.

Customers who cannot provide the standard evidence

2.4.7 Where a bank concludes that an individual customer cannot reasonably meet the standard identification requirement[33] it may accept as identification evidence a letter or statement from an appropriate person who knows the individual, that indicates that

.....

[33] The EBA has issued an 'Opinion on the application of Customer Due Diligence Measures to customers who are asylum seekers from higher risk third countries or territories', see https://eba.europa.eu/documents/10180/1359456/EBA-Op2016-07+%28Opinion+on+Customer+Due+Diligence+on+Asylum+Seekers%29.pdf.

the person is who he says he is. Alternative methods can be used to verify the person's identity.

Directive (EU) 2014/92

2.4.8 In the Netherlands[34] every adult needs his own payment account to be able to participate in society. The banks and social work agencies have therefore agreed that everyone in the Netherlands over 18 years of age with a known address must be able to open a payment account. To this end, in 2001 the Dutch Banking Association (NVB), the Ministry of Finance and the Salvation Army agreed on the 'Covenant on a package of primary payment services', also known as the 'Covenant on a Basic Bank Account'.

Documentary evidence

Wwft 11(4) (1)

2.4.9 If documentary evidence of an individual's identity is to provide a high level of confidence, it will typically have been issued by a government department or agency, or by a court or local authority, because there is a greater likelihood that the authorities will have checked the existence and characteristics of the persons concerned. In cases where such documentary evidence of identity may not be available to an individual, other evidence of identity may give the bank reasonable confidence in the customer's identity, although the bank should weigh these against the risks involved. These alternative methods could be included in a local risk assessment.

Implemetation regulation 4 (1)

The identity of natural persons can be verified by means of "documents, data or information from reliable source independent of the customer". Without being exhaustive article 4(1) of the Implementation Regulation of the Wwft mentions:

- A valid passport;
- A valid Dutch identity card;
- A valid identity card issued by the competent authority in another Member State and bearing a passport photo and the name of the holder;
- A valid Dutch driving license;

.....

[34] In the Netherlands, this right was enshrined in the Financial Supervision Act (Wft) in 2016 via the Implementation Act on access to a basic payment account. This necessitated amendments to the Covenant on Basic Bank Accounts. The Covenant was based on self-regulation; after all, until 2016 there was no statutory right to a basic payment account in the Netherlands, as there has been for most EU citizens since then. https://www.basisbankrekening.nl/achtergrond/uitleg/

- A valid driving license issued by the competent authority in another Member State and bearing a passport photo and the name of the holder;
- Travel documents for refugees and foreign nationals;
- Residence permit, issued on the basis of the Aliens Act 2000.

Other considerations

Persons acting towards the bank on behalf of the customer (private individual)

Wwft 3 (2e) (3)

2.4.10 If the customer is represented by a natural person, the Wwft requires that this representative is identified, and his identity is verified. The bank needs to determine whether the relevant person is authorised to represent the customer.

The most commonly authorised representatives (by force of law or by proxy) are:

- Parent or guardian;
  Guardianship is the custody of minor children that is not exercised by the parents, but by someone else: the guardian. This can be either a natural person or a legal entity (guardianship institution). As soon as the minor reaches the age of majority, he or she must be registered as a new, independent customer and the guardianship of the guardian will lapse;
- Representative appointed by court order (“curator/ bewindvoerder”);
- Notarial Attorney (“notarieel gevolmachtigde”);
  The natural person who is listed as a proxy on behalf of the customer in a power of attorney (notarial power of attorney) laid down by a notary public;
- Representative authorised otherwise by the private individual to act on his behalf.

Wwft 3 (3)

2.4.11 The representative of a customer (private individual) who acts on the customer’s behalf must be identified and his identity must be verified. The following information and documentation need to be recorded in the customer file:

- Full name (given name(s) and surname(s));
- Date of birth.

Refer for the verification of the representative to 2.4.4 – 2.4.9

Minors

2.4.12 Often a customer relationship in respect of a minor will be established by a parent or guardian. In cases where the adult opening the account or establishing the relationship does not already have an existing relationship with the bank, the identity of that adult[35] must be verified, unless there is a strong suspicion that the person is not the parent. In that case, if there are any doubts, the bank must request a copy of the birth register or Marriage Act. It is also possible to ask the person concerned for an up-to-date extract from the authority register (gezagsregister). The minor must then have his or her identity verified in person before or upon reaching age of majority (18), by means of his or her own identity card.

2.4.13 Identification and verification of the underage customer can take place in two ways:

1. The minor himself or herself appears in person with his or her own identity document, this is identification and verification in person of the minor himself or herself, in addition, the ID of the parent or guardian must also always be verified.
2. Identification and verification of the minor is done by the parent or guardian using the identity document of the parent or guardian.

In the second case, the identification and verification has a limited shelf life: the minor will have to have his or her identity verified in person with his or her own identity card before reaching majority (18 years).

In the Netherlands, minors must have their own identity documents from the age of 14. In addition, minors must have their own proof of identity when travelling abroad.

2.5 Customers other than private individuals - entities

2.5.1 Depending on the nature of the entity, a relationship or transaction with a customer, who is not a private individual, may be entered into in the customer's own name, or in that of specific

[35] For the parents/legal representatives of minor clients, it is sufficient to provide personal data of the minor combined with an explicit declaration by the parent that as parent and legal representative he is authorised to represent the minor, unless there is a strong suspicion that the person is not the parent. If the bank doubts the authority to represent, relevant documents must be requested to verify the authority.

individuals or other entities on their behalf. Beneficial ownership may, however, rest with others, either because the legal owner is acting for the beneficial owner, or because there is a legal obligation for the ownership to be registered in a particular way.

2.5.2 In this Guidance an entity is described as follows: an entity other than a natural person that can establish a permanent customer relationship with a bank or otherwise own property. This can include limited liability companies, (private /limited) partnerships, trusts or other similar legal arrangements. This section provides guidance on verifying the identity of a range of entities.

2.5.3 This section provides guidance on identifying and verifying the identity of the following range of entities:

- Corporate entities including their (in)directly 100%-owned subsidiaries;
- Regulated credit and financial institutions;
- Government institutions;
- Religious bodies;
- Other entities e.g. foundations, associations, mutual benefit associations and cooperatives;
- Partnerships:
    - General partnership (“vennootschap onder firma/VOF”);
    - Professional partnership (“maatschap”);
    - Limited partnership (“Commanditaire vennootschap/CV”);
- Trusts and similair legal arrangements.

2.5.4 Banks may take a risk-based approach when determining the extent of the CDD measures. Some of the types of customers listed above may entail a lower ML/TF risk. If the risks associated with the customer are low SDD, also known as adjusted CDD, may be applied. SDD is not an exemption from any of the CDD measures; however, banks may adjust the amount, timing or type of each or all of the CDD measures in a way that is commensurate to the identified low risk. Refer to paragraphs 1.5.20-1.5.28 for more information on SDD/adjusted due diligence.

Wwft 33 (2) sub c

2.5.6 For entities as customer, the following details are recorded:

- Full legal name;
- Trading name(s) where applicable;

- Legal form;
- Proof of existence;
- Registered address or legal seat in country of incorporation or organization (including street and number, postal code and country of registered office);
- Principal place of business address if different from registered address;
- Registration number at the Chamber of Commerce (or alternatively the company legal identification number, if there is no registration number at the Chamber of Commerce).
- the representatives of a customer and their i) full name and ii) date of birth.

Wwft 11(3)

2.5.7 The information must be verified based on documents, data and/or information from a reliable and independent source. The bank must be able to argue that it was justified to rely on the used documents, data or information. For customers incorporated under Dutch law, this will in principle be an extract from the Chamber of Commerce. For customers incorporated in other countries, the source is likely to be the national or local corporate registry or other locally acceptable documentation.

Implementation regulation Wwft 1(2)

2.5.8 Article 4, second paragraph, of the Implementing Regulation of the Wwft states the following (not limitative) list of sources that can be used:

Dutch and foreign entities, established in the Netherlands:

- (electronic) commercial register extract (option: certified);
- a deed or statement by a Dutch notary or a comparable official from another Member State.

Foreign entities, not established in the Netherlands:

- documents from independent sources, data or information which are reliable and commonly used in the international course of business (e.g. company register);
- documents, data or information recognised by law as valid means of identification in the customer's country of origin (e.g. a copy of the certificate of incorporation).

Other customers:

- On the basis of documents, data or information from reliable and independent sources.

2.5.9 Registration in the trade register of the Dutch Chamber of Commerce is also mandatory for a subsidiary or branch of a foreign legal entity in the Netherlands. In the case of a subsidiary, the information in the trade register will relate to that subsidiary as a separate legal entity. A branch has, as part of the foreign legal entity, the same legal form as the foreign legal entity.

2.5.10 Information relating to foreign legal entities can (also) be obtained through the trade register in the country of incorporation, through the public UBO register[36] or through a statement from a lawyer, notary or comparable independent legal service provider. A bank can, where appropriate, take into account the reputation of the service provider concerned and any risks associated with the relevant country, including possible shortcomings in the legal trade register regime. In order to investigate such risks, an institution can consult reports from authoritative international organizations, such as the Financial Action Task Force.

*Wwft 8(5), 9(1)*2.5.11 If an entity is known to be linked to a PEP (as a result of the PEP being a beneficial owner of the entity), or to a jurisdiction assessed as carrying a higher ML /TF risk, enhanced due diligence measures must be applied.

Identification and verification of the UBO

2.5.12 When deciding who the beneficial owner is in relation to a customer who is not a private individual, the bank's objective must be to know who has ownership or control over the funds, which form or are otherwise connected to the relationship, and/or form the controlling mind and/or management of any entity involved in the funds. Verifying the identity of the beneficial owner(s) will be carried out on a risk-based approach and will take account of the number of individuals, the nature and distribution of their interests in the entity and the nature and extent of any business, contractual or family relationship between them (refer to paragraphs 2.3.23 – 2.3.32).

Identification of effective control

2.5.13 Apart from the UBOs that have an ownership or control interest, there may be situations where non-identified individuals may exercise effective control over the customer through other means. FATF gives the following description of effective control:

.....

[36] Under the Fourth Money Laundering Directive, all European Member States are required to set up a central register of information on UBOs of companies and other legal entities.
https://www.rijksoverheid.nl/onderwerpen/financiele-sector/ubo-register

1. Shareholders who exercise control alone or together with other shareholders, including through any contract, understanding, relationship, intermediary or tiered entity (a majority interest approach). This indirect control could be identified through various means, as shareholder's agreement, exercise of dominant influence or power to appoint senior management. Shareholders may thus collaborate to increase the level of control by a person through formal or informal agreements, or through the use of nominee shareholders. It is necessary to consider various types of ownership interests and the possibilities that exist within a particular country, including voting or economic rights. Other issues worth considering are whether the company has issued convertible stock or has any outstanding debt that is convertible into voting equity.
2. The natural person(s) who exert(s) control of a legal person through other means such as personal connections to persons in positions described above or that possess ownership.
3. The natural person(s) who exert(s) control without ownership by participating in the financing of the enterprise, or because of close and intimate family relationships, historical or contractual associations, or if a company defaults on certain payments.

Furthermore, control may be presumed even if control is never actually exercised, such as using, enjoying or benefiting from the assets owned by the legal person.

Examples of other situations where ownership does not equal control are described in Annex 2-II.

As effective control may not have been fully identified during the (enhanced) due diligence process, banks should request the customer on a risk-based approach to confirm whether there are other UBOs that have effective control.

Understanding the ownership and control structure

Legal requirements and industry standards

WWft 3 (2)(b)

2.5.14 Banks must take reasonable steps to understand the ownership and control structure of a customer.

DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act 4.3

2.5.15 Banks must also have reasonable measures in place to provide an insight into the customer's ownership and control structure in the case of legal persons, trusts and other legal arrangements. This includes measures to verify the legal status of customers other than natural persons, if possible by obtaining proof of incorporation. The basic principle is that the bank knows the relevant structure, and understands it. This means that for complex structures consisting of many companies, the bank must devote more efforts to understand the domestic and/or (international) shareholder and control structure of the entity than for a Dutch private limited company (BV) with a majority shareholder-director. As part of these efforts, the bank examines the customer's reasons for using complex structures. This can be achieved by inquiring with the customer, but also by requiring a legal or tax opinion or advice.

ESAs Guidelines on risk factors – Customer risk factors

2.5.16 A factor that may contribute to increasing the risk is when the customer's beneficial owner cannot be easily identified, for example because the customer's ownership structure is unusual, unduly complex or opaque, or because the customer issues bearer shares.

ESAs Guidelines on risk factors – Enhanced CDD

2.5.17 Therefore, an EDD measure that may be appropriate in high-risk situations is to ensure that the bank is satisfied that a customer's use of complex business structures such as trusts and private investment vehicles is for legitimate and genuine purposes only, and that the identity of the ultimate beneficial owner is understood.

FATF Guidance on Transparency and Beneficial Ownership

2.5.18 For example, beneficial ownership information can be obscured by the use of:

- Shell companies (which can be established with various forms of ownership structure), especially in cases where there is foreign ownership, which is spread across jurisdictions;

- Complex ownership and control structures involving many layers of shares registered in the name of other legal persons;
- Bearer shares and bearer share warrants;
- Unrestricted use of legal persons as directors;
- Formal nominee shareholders and directors where the identity of the nominator is undisclosed;
- Informal nominee shareholders and directors, such as close associates and family;
- Trusts and other legal arrangements that enable a separation of legal ownership and beneficial ownership of assets;
- Use of intermediaries in forming legal persons, including professional intermediaries.

Identification of complex structures

2.5.19 The ownership and control structure of a customer refers to the trail of all involved legal entities and/or arrangements starting from the customer legal entity/arrangement leading up to the UBO(s).

2.5.20 Such structures can consist of many layers of intermediate parents. Besides the number of layers between the customer and its UBOs, there can be complex entities like trusts and other similar legal arrangements in the structure. Control can be further obscured through the use of shares that hold different or no voting rights, by granting usufruct of shares as well as pledging them. Finally there can be individuals exercising effective control over an entity through other means than through formal ownership, (e.g. agreement between shareholders, the use of nominee shareholders, etc.).

2.5.21 All these factors can lead to difficulty in ascertaining the actual UBO of the customer. Banks have a legal obligation to understand the ownership and control structure of a customer and to take reasonable measures to verify such structures.

2.5.22 However, a complex structure in itself does not necessarily indicate ML/F. The reasons for such structures may be legitimate and will likely be tax related. However, these structures can also be used to hide the actual ownership of a customer, to obscure the purpose of the relationship or the source of funds or to facilitate tax evasion.

2.5.23 The following situations are red flags for complex structures and will require appropriate EDD measures:

- A structure consisting of more than 4 layers of ownership from the customer up to the UBO (where the customer and the UBOs are each considered to be a separate layer). Structures with more than 4 layers are not considered complex in case:
  - All intermediate parent companies are incorporated in the same country (low and medium risk countries only) as the customer; and
  - The UBOs are resident in the same country as thecustomerthe customer; and
  - There are no complex entities in the structure; and
  - No other red flags for complex structures are present; and
  - The structure matches the profile of the customer.
- The structure contains companies that have been incorporated in non-transparent jurisdictions;
- Knowledge of presence of bearer shares and bearer share warrants in the structure;
- Presence of trusts or similar legal arrangements in the structure;
- Nominee shareholders and directors in the structure where the identity of the actual beneficial owner is undisclosed.

2.5.24 EDD on complex structures will not be required for Recognised Exchange listed entities, Recognised Regulated entities and state-owned enterprises.

2.5.25 Privately-held multinationals may have complex structures by their very nature . EDD is not required if , , there is a great deal of public information available on such entities. However, some caution needs to be exercised and in case specific red flags have been identified regarding the ownership and control structure of the privately-held multinational (e.g. material adverse media regarding the legitimacy of the structure or tax evasion), then EDD will be required as for other entities.

Enhanced Due Diligence measures for complex structures and effective control

2.5.26 In case EDD is applied (as described in the paragraphs above), the measures that apply to all complex structures always include:

- Identification of the ownership and control structure of the customer and verification through reliable sources;

- Identification of the immediate and intermediate parents and risk-based verification of their legal existence through reliable sources;
- Justification by the client of the use of such a structure in case it does not match its profile and/or does not have any apparent economic purpose.

In certain cases it may also be appropriate to request an opinion or advice from a tax specialist (either internal or external) on the tax risks that were identified in the structure.

Specific measures apply for the following situations:

2.5.27 *Shell companies and non-transparent jurisdictions.*
Ownership and control structures involving non-transparent jurisdictions require EDD measures due to the heightened risk of tax evasion and obscuring the trail to the UBOs. EDD measures may include verification of legal existence and/or an opinion from an internal or external tax specialist.

If the customer itself is a shell company, the bank could pay close attention to the nature and purpose of the relation, as well as have a thorough understanding of the source of funds used for the transactions. On a risk-based approach it may be necessary to have insight into the structure "underneath" as the source of funds may be from complex structures.

2.5.28 *Bearer shares*
Establishing a relationship with customers where bearer shares have been identified in the structure can be allowed if the holders of all outstanding shares are identified by means of:

- Converting them into registered shares (for example through dematerialisation); or
- Immobilising them by requiring them to be held in custody with a Recognised Regulated entity or a professional intermediary regulated by a Recognised Regulator.The bank must receive an official statement from the custodian stating the details of the UBOs holding the shares and verify their identity. The custodian must also state that it will inform the bank immediately of any change in ownership or in case the shares are withdrawn from custody;

Note that the requirements below do not apply to bearer shares issued by Recognised Exchange listed entities.

In case of existing customers that refuse or have no power to dematerialise or to immobilise the bearer shares, banks may:

- Receive an official statement about the reasons for not dematerialising or immobilising the bearer shares as well as the details of the beneficial owners; and
- Verify whether local applicable laws require private individuals owning more than 10% of the shares to notify the company and the company to record their identity and the company will inform the bank immediately of any change in ownership.

2.5.29 Complex entities in the structure
An ownership structure involving complex entities will require different approaches, depending on the type of entity that is used. The definition of a UBO may differ for each of these entities. See identification and verification of the UBOs 2.3.23 – 2.3.32.

2.5.30 *(In)formal nominee shareholders and directors in the structure*
The presence of nominee shareholders does not always constitute a red flag. In some countries there may be restrictions with respect to foreign ownership of local companies. In such cases, foreign holdings make use of local residents to hold shares on their behalf.

Where shares are held by nominee shareholders, banks could identify and verify the actual ultimate beneficial shareholders to whom these entities or persons provide nominee services, as opposed to identifying the UBOs of the nominee shareholder (where this is an entity).

(i) In case of *nominee shareholders*, i.e. TCSPs, lawyers or other professional service providers that provide nominee services to third parties, at least the following information and documents may be obtained:

- A statement from the regulated nominee shareholder confirming whether there are any UBOs holding more than 25%, as well as the details of those UBO(s), including type and percentage of shares; and
- A copy of the underlying contracts for the provision of nominee services/custodial agreement (not required if the nominee shareholder is regulated by a Recognised Regulator

or otherwise subject to the AML/CTF legislation of an Equivalent Country); and
- A justification for the use of nominee shareholders from the customer or the UBO.

(ii) In case the customer makes use of *nominee directors* at least the following information and documents maybe obtained:

- A statement from the service provider with the details of all proxy holders and their powers;
- Copy of the underlying contracts for the provision of nominee services (not required if the nominee director is regulated by a Recognised Regulator or otherwise subject to the AML/CTF legislation of an equivalent country);
- A justification for the use of nominee directors from the customer.

(iii) In *other cases* of other legal entities as directors:
- Obtain the power of attorney of the natural persons that represent the legal entity directly or indirectly in its capacity as director of the customer;
- In case the legal entity director again has a legal entity as director, the customer could provide a justification for such a structure.

Identification and verification of representative(s) and director(s)

Identification and verification of representative(s)

Wwft 3(2)(e), (3), (4)

2.5.31 Customers other than natural persons are represented by one or more natural persons. Banks should take appropriate steps to be reasonably satisfied and be confident that the person they are dealing with is properly authorised to represent the customer. The adequate representation must be established and verified to obtain transparency, not only to prevent ML/TF risks. Misrepresentation is a legal risk and it may be a fraud risk. Therefore it must be independently established whether the person representing the customer currently has a formal role with that entity (has been duly appointed and not been discharged); and whether, in that role, that person may face the bank on behalf of that entity.

2.5.32 Where a natural person claims to indirectly represent an entity, the chain of representative authority needs to be established.

Wwft 3(2)(e), (11), 11(1)

2.5.33 Banks must verify the identity of authorised persons based on reliable and independent documentation, data or information. The nature and the extent of the information required for verification depends on the risks involved, including the type of customer, the nature of the relationship, the product or the transaction (see 2.4).

2.5.34 There are the following categories of authorised representatives:

1. *Direct appointees/authorised representatives by force of law:* These persons represent the customer towards the bank at customer relationship level in general and are legally authorised by statutory provision, articles of association or by relevant law. These include company directors, the company secretary, the trustee, managing partners, etc.
2. *Authorised representatives by proxy:* These persons represent the customer towards the bank at customer relationship level concerning dedicated legal responsibilities and are delegated by the direct appointees to represent the customer, either for the entire relationship or for a specific product or service: These include authorised signatories, proxy holders, holders of a power of attorney, etc.

Wwft 3(8)(9)

2.5.35 In case of large corporate customers different persons may act towards the bank depending on the products requested (e.g. loans, forex, markets, products). The verification of the authorisation of such a person to represent the customer and the verification of the identity may take place as part of the product process. The bank should take care that relevant documentation is available through the CDD file of the customer. Banks do not have to re-establish this information during a regular CCD-review but process updates as an event driven review (e.g. renewal of a loan agreement).

Paragraph 4.1.3 DNB Guidance AML/CTF and SW

2.5.36 For operational staff who during the existence of the relationship with an entity may act towards the bank for specific activities, e.g. the execution of payment orders, it is sufficient for the bank to verify whether they are authorised by the entity to do so. This can be established without verification of identity of those persons. In those circumstances it is sufficient for the bank to establish the capacity of those persons to bind the entity for the specific activity and to recognise them as such in the exercise of this capacity as

agreed with the customer. The means to recognise the capacity of such persons are a.o. the use of a (bank)card and (PIN)code or a specimen of the authorised signature provided by the entity.

2.5.37 The Wwft does not specify how banks should examine whether the representative is duly authorised to represent the client, except that banks may determine the extent of such measures on a risk-based approach. This means that depending on the circumstances independent and reliance sources are used in determining an authorised representative's power to represent. A bank needs to determine how it may comply with this obligation. In practice, this means that banks have to request a power of attorney or need to check the Trade Register of the Chambers of Commerce. All data collected during the CDD process must be recorded in a readily retrievable way.

Identification of director(s) who are not acting towards the bank

2.5.38 As part of their risk-based approach banks may consider to record one or more directors for screening purposes .

Corporate entities

2.5.39 Corporate entities and their (in)directly 100%-owned subsidiaries may be publicly accountable in several ways. Some public companies are listed on stock exchanges or other regulated markets, and are subject to market regulation and to a high level of public disclosure in relation to their ownership and business activities. Other public companies are unlisted, but are still subject to a high level of disclosure through public filing obligations. Private companies are not generally subject to the same level of disclosure, although they may often have public filing obligations. In their verification processes, banks should take account of the availability of public information in respect of different types of company.

2.5.40 A public limited company, or in Dutch *een naamloze venootschap* (NV), is a company whose capital is divided into shares in a similar way to that of a private limited company (besloten vennootschap, BV). An NV issues registered shares, but also shares that can be freely traded on the stock exchange, whereas a BV can only issue registered shares transferable by a civil-law notary. Both BVs and NVs have to issue and file their annual reports and accounts with the Chamber of Commerce. The size

and scale of the company determines exactly how this should be carried out.

2.5.41 The structure, ownership, purpose and activities of the great majority of corporates will be clear and understandable. Corporate entities can use complex ownership structures, which can increase the steps that need to be taken to be reasonably satisfied as to their identities; this does not necessarily indicate ML/TF. The use of complex structures without an obvious legitimate commercial purpose may, however, give rise to concern and increase the risk of ML/TF. Refer to 2.5.26 – 2.5.30 for more information about complex structures.

2.5.42 Control over companies may be exercised through a direct shareholding or through intermediate holding companies. Control may also rest with those who have power to manage funds or transactions without requiring specific authority to do so, and who would be in a position to override internal procedures and control mechanisms. Banks should make an evaluation of the effective distribution of control in each case. What constitutes control for this purpose will depend on the nature of the company, the distribution of shareholdings, and the nature and extent of any business or family connections between the beneficial owners.

2.5.43 To the extent consistent with the risks involved the bank may consider to take reasonable measures to understand the company's legal form and ownership and control structure, and must obtain sufficient additional information on the nature of the company's business, and the reasons for seeking the product of service.

Wwft 3(2)b

2.5.44 In case of corporates, a UBO is defined as natural person(s) either owning or controlling more than 25% of the corporation or otherwise owning or controlling the customer. These natural person(s) must be identified, and reasonable measures must be taken to verify their identities. The UBO definition includes at least:

1. A natural person(s) who ultimately directly or indirectly own(s) more than 25% of the shares in the share capital of a legal entity;
2. A natural person(s) who ultimately hold(s) more than 25% in voting rights in the meeting of shareholders of a legal entity;

3. A natural person(s) who ultimately directly or indirectly own(s) more than 25% interest or profit share in a legal entity; or
4. A natural person(s) who otherwise exercises effective control.

If no UBO is identified under 1 to 4 above the natural person(s) who, either directly or within the group to which the customer belongs, exercises effective control based on the responsibility for the strategic decisions that fundamentally affect the daily or regular affairs/business practices of the customer, is/are identified as UBO(s).

2.5.45 In case (a) no UBO is identified under 2.5.44 and there are no grounds for suspicion; or (b) in cases of doubt, where there is uncertainty whether the person or persons identified are in fact UBO, a natural person(s) who hold(s) the position of senior managing official(s) are classified as UBO. Please note that identifying a senior managing official as UBO can only be done as a last resort when there are no grounds for suspicions and in case of doubt.

2.5.46 Normally, if a UBO is established for a customercustomer that holds more than 25% of the shares, or is the ultimate owner or exercises effective control in any other way, this is in principle also the UBO of the operating companies that are 100% owned by the customer; of course this is always in sofar as there are no indications that the operating company has another UBO. However, if the senior managing official statutory is identified as UBO as no UBO could be identified under the definition as stated under 2.5.44, then this senior managing official of the customer is not automatically also the UBO of the operating company. In that situation the senior managing official of the operating company should be deemed the UBO, unless there is actual knowledge that there is a different UBO.

2.5.47 Banks might want to consider to adopt a lower threshold than the more than 25% stated in 2.5.44 in certain cases that present a particular high risk to the bank. This is particularly the case if the bank is not reasonably satisfied that it knows who the UBO is, for example where the customer's ownership and control structure is not transparent and/or does not make sense and/or if the customer's ownership and control structure is complex or opaque and there is not an obvious commercial or lawful rationale.

2.5.48 In order to verify the director/100% - shareholder of a corporate as a UBO an extract from the Dutch Chamber of Commerce which states the name of the 100%-shareholder can be used.

Corporate entities listed on a Recognised Exchange

Directive (EU) 2015/849

2.5.49 Public companies, including their 100%-subsidiaries, listed on stock exchanges or other regulated markets are subject to market regulation and to a high level of public disclosure with regard to their ownership and business activities. Therefore these customer relationships may present a low degree of ML/TF risk and simplified CDD measures may be applied (refer to Annex II to Directive (EU) 2015/849). In determining whether a customer relationship presents a lower degree of ML/TF risk and therefore simplified CDD may be applied, a bank must:

- Establish and document whether the customer is a company whose securities are admitted to trading on a Recognised Exchange or is an 100%-owned subsidiary of such a listed company (refer to the list of Recognised Exchanges for an overview of these markets); and
- Carry out an appropriate risk assessment on the customer and establish that there are no indications of higher risks.

The bank must record the above-mentioned assessment and the steps it has taken to verify the fact that the customer is listed on a Recognised Exchange. Refer to paragraphs 1.5.20 – 1.5.28 for more information on SDD/adjusted due diligence.

2.5.50 If it is established that a lower level of CDD measures (SDD) may be applied, there is no need to identify any directors (unless they are acting towards the bank) and the bank can adjust the intensity of the verification measures with regard to the authorised representative in quantity, quality and timing. This is related to the determination to act and to the verification of the identity of the authorised representative.

Implementing Decree Wwft 2018 3(1)(a)

2.5.51 If the customer is a company listed on a Recognized Exchange, there is an exemption under Dutch law to identify and verify the UBO(s). Given the fact that there is no legal obligation to identify the UBOs of these customers, the general assumption is that there is also no obligation to identify the senior managing official. This equally applies to non-listed entities that are a (in)direct 100% subsidiary of a listed company on a Recognized Exchange.

This legal exemption applies regardless of the overall risk rating of the customer.

2.5.52 In more developed markets, in general the bank can expect fragmented ownership in the case of listed companies on a Recognized Exchange, but especially in less developed markets the ownership might not be as fragmented yet; for example because in case of family owned entities families do not sell out or families are still in the process of selling out over time as a general theme. In those situations or similar situations, it is best practice that the ownership- and control structure of such listed companies on a Recognized Exchange are described.

Regulated credit and financial institutions

FATF 40 Recommendations

2.5.53 FATF mentions in the 40 Recommendations as a possible area of lower risk customers credit and financial institutions that are already subject to requirements to combat ML/TF consistent with the FATF Recommendations, and that have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements. These credit and financial institutions pose less risk from a ML/TF perspective than a customer that is unregulated or subject only to minimal AML/CTF regulation. In determining whether a customer relationship presents a lower degree of MLTF risk and therefore SDD may be applied, a bank must:

- Establish that the customer is a credit or financial institution which is subject to the requirements listed above (e.g. by consulting applicable (public) registers); and
- Carry out an appropriate risk assessment on the customer and establish that there are no indications of higher risks.

The bank must record the above-mentioned assessment and the steps it has taken to check the regulatory status of the regulated credit and financial institution. Refer to paragraphs 1.5.20 -1.5.28 for more information on SDD/adjusted due diligence.

2.5.54 If it is established that SDD may be applied there is no need to identify any directors (unless they are acting towards the bank)

and the bank can adjust the intensity of the verification measures with regard to the authorised representative in quantity, quality and timing. This relates to the determination to act and to the verification of the identity of the authorised representative.

Government institutions

Directive (EU) 2015/849 Annex II

2.5.55 Banks may take a risk-based approach when determining the extent of the CDD measures taking into account the risk factors listed in Annex II to Directive (EU) 2015/849. Public authorities and local governments are listed on this non-limitative list of lower risk factors. If the ML/TF risk associated with the customer relationship or the occasional transaction is low, simplified CDD measures may be applied.

Wwft 2(b)2

2.5.56 With respect to customers which are Dutch or overseas governments (or their representatives), supranational organisations, government departments, state-owned companies or local authorities, the approach to identification and verification may be tailored to the circumstances of the customer, reflecting the bank's determination of the level of ML/TF risk presented. Where the bank determines that the customer relationship presents a low degree of risk of ML/TF, simplified CDD measures may be applied. Banks must carry out an appropriate risk assessment on the customer and establish that there are no indications of higher risks. This assessment must be recorded. Refer to paragraphs 1.5.20-1.5.28 for more information on SDD/adjusted due diligence.

2.5.57 For the question whether UBO-requirements apply to a government institution, it is important to understand that part of the UBO requirements is that the bank also establishes the legal status (legal personality) of customers who are not natural persons, if possible by obtaining proof of establishment. The term legal entity includes legal entities such as private companies and entities on a contractual basis such as partnerships. The obligation to register in the trade register of the Dutch Chamber of Commerce applies to both.

2.5.58 When the government institution is organized as a public-law entity (government, municipality, provinces, etcetera), the UBO requirements only apply in case of totalitarian regimes. There is a chance that those in power will abuse their position for their own gain and are in fact the UBO. If that is the case, CDD measures

must be applied in line with the enhanced CDD measures applicable to PEPs.

2.5.59 In case a private company (for example, a private limited liability company or another legal entity under private law) that is partially or wholly owned by the government, the UBO is determined in the manner described above. Also in this context, in case of totalitarian regimes the risk that those in power will abuse their position for their own gain and in fact their capacity as UBO should be assessed, just as it should be determined if that is indeed the case.

Dutch public authorities

2.5.60 Public authorities engaged in public administration are generally incorporated by law and often set up in different forms. It should be established that the customer is part of the Dutch government and verified that the public authority exists. This can, for example, be done by means of an extract of the Chamber of Commerce register and from official government websites. A Dutch public authority can be defined as any Dutch national, provincial or municipal government body with public duties and competences pertaining to public law. This includes, but is not limited to:

- The Dutch government;
- Ministries (responsible for a sector of government public administration, that can have responsibility for one or more departments, agencies, bureaus, commissions or other executive, advisory, managerial or administrative organisations in relation to public duties);
- High Councils of State (the Netherlands Court of Audit, the Senate, the House of Representatives, the Council of State, the National Ombudsman);
- Public bodies for the professions and trades and other public bodies;
- Provincial bodies (e.g. College of the King's Commissioner, Provincial Council);
- Municipalities (e.g. the College of Mayor and Alderpersons, City council);
- The judicial system;
- Dutch regional water authorities (“waterschappen” or “hoogheemraadschappen”).

2.5.61 Embassies in the Netherlands are considered ‘foreign public authorities’ and should be treated as such.

Dutch semi-public authorities

2.5.62 Dutch semi-public authorities are not fully government owned, whereby the ownership and control structure needs to be recorded in the customer file. Examples are public broadcasters, national museums, public libraries, education institutions and healthcare services and utility companies.

Supra- or international organisations

2.5.63 International organisations are entities established by formal political agreements between their member states that have the status of international treaties; their existence is recognized by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organizations include the United Nations and affiliated international organizations such as the International Maritime Organization; regional international organizations such as the Council of Europe, institutions of the European Union, the Organization for Security and Co-operation in Europe and the Organization of American States; military international organizations such as the North Atlantic Treaty Organization, and economic organizations such as the World Trade Organization or the Association of Southeast Asian Nations, etc.

2.5.64 Similar to public authorities the CDD on supra- or international organisations must be adjusted to the risks involved. The available documentation, data or information may vary depending on the jurisdiction of the foreign public authority and supra- or international organisations.

Religious bodies

2.5.65 A religious body (“kerkgenootschap”) is an organisation that aims to make people with the same religion live their faith together. It is not only about (Christian) churches, but also about places of worship and institutions affiliated with all possible beliefs or groups that are so popular. A religious body, as a legal form, is often divided into an umbrella organisation or diocese ('head office') and associated units (individual churches,

seminars, parishes, etc.). Apart from religious bodies a religious organisation can also be established in another legal form, such as a foundation.

2.5.66 Religious bodies can have a higher ML/TF risk because of the large number of (cash) donations by mostly unknown parties. In addition, the organisation may be used for other activities than just religious purposes or even only have religion as a cover for other activities. Examples are TF, but also ML and tax fraud. Given that religious bodies could potentially have connections with high-risk countries and / or conflict areas (e.g. missionary work), this gives an extra risk of involvement in financing terrorism in those countries, as well as violation of sanctions legislation. Finally, a religious body is not a protected concept and can in theory be established by everyone. Religious bodies can therefore have a higher integrity risk.

2.5.67 Religious bodies may have an ANBI ("Algemeen Nut Beogende Instellingen") status. This status is granted by the Dutch tax authorities, if an organisation meets the applicable conditions. For the Roman Catholic denomination, for example, the tax authorities issued a group decision in which the Roman Catholic Church and all its independent units have been designated as ANBI. This may also be the case for other religious organizations. A Dutch religious body may also be affiliated with the interdenominational contact in government affairs (CIO http://www.cioweb.nl/).

FATF RECOMMENDATION 8

2.5.68 Banks should take into account that FATF and the Office of Foreign Assets Control (OFAC) have issued specific guidance on these type of organisations and the higher risk that can be associated with them.

2.5.69 Registration at the Chamber of Commerce is mandatory for religious bodies, unless they are part of an umbrella organisation. If the denomination is registered at the Chamber of Commerce (headquarters), an excerpt of this is sufficient for the verification of the customer. If the denomination is not registered in the trade register (branch offices), a denomination declaration could be issued.

The existence of other religious organisations can be verified from a number of different sources, depending on the legal form of the organisation and whether it is registered or not.

2.5.70 In case of a religious body the UBO is/are the natural person(s) who ha(s)(ve) been appointed as legal successor(s) in the statute of the organisation upon dissolution of the organisation. If (a) based on this rule no UBO can be identified and there are no grounds for suspicion; or (b) in cases of doubt, where there is uncertainty whether the person or persons identified are in fact UBO the natural person(s) appointed in the statute/documentation of the organisation as the members of the executive committee of the in the governing body are identified as UBO(s).

Implementing Decree Wwft 2018 3(2)(2)

2.5.71 To identify the representatives of a religious body, banks should have a declaration of the religious body, articles of association and/or appointment decisions. This also applies if the denomination is registered with the Chamber of Commerce, but the representatives are not registered with the Chamber of Commerce. In addition, the power of attorney of the umbrella organisation (e.g. the Diocese), to which the religious body concerned is affiliated, is also required for the 'founder' of the branch, so that it is clear whether the latter may act on behalf of the Diocese and/or is affiliated to it.

Other legal entities

2.5.72 For the Dutch foundations, associations, mutual benefit associations and cooperatives the UBO is defined as any natural person(s):

1. Who directly or indirectly holds more than 25% of ownership;
2. Who in decision-making with regard to amendments of the articles of association has the ability to exercise more than 25% of the voting rights;
3. Who has effective control over the entity.

If no UBO is identified under 1 to 3 above, the natural person(s) who exercise effective control based on the responsibility for the strategic decisions that fundamentally affect the daily or regular affairs/business practices of the customer, is/are identified as UBO(s).

2.5.73 In case (a) no UBO is identified under 2.5.72 and there are no grounds for suspicion; or (b) in cases of doubt, where there is

uncertainty whether the person or persons identified are in fact UBO, a natural person(s) who hold(s) the position of senior managing official(s) is/are classified as UBO. Please note that identifying a senior managing official as UBO can only be done as a last resort, when there are no grounds for suspicions and in case of doubt.

Foundations

2.5.74 A foundation (in Dutch “stichting”) is a legal entity, which means that its officers are theoretically not liable for any of its debts. There are, however, exceptions to this rule; for example, mismanagement, negligence or failure to list the foundation in the Commercial Register. A civil-law notary is needed to draft a deed, stating that the foundation is set up and listing its statutes. Statutes often also include rules about the foundation's organisation. Information about the organisation and control structure can also be derived from the notarial deed. It is also possible to set up a foundation with other individuals and/or entities e.g. a so-called BV. In the Netherlands it is mandatory to register the foundation with the Commercial Register maintained by the Chamber of Commerce but does not has any legal obligation to deposit financial statements regarding to the foundation.

2.5.75 A foundation has a board, but no members. When a foundation only has one board member this may pose a potential higher risk. It may also be a business, but its profits must be allocated to the foundation's cause or purpose. The foundation's officers can even be paid employees, although this is not often the case. Generally speaking, officers only receive remuneration for their expenses. Non-profit or charitable organisations are often foundations. These organisations fulfil an important social and societal role within society. They are primarily engaged in raising funds for a specific purpose such as social support, religion, culture, education or other 'good causes'.

FATF Recommendations 8

2.5.76 In assessing the risks presented by NPO’s , a bank may consider to distinguish between those with a limited geographical range, and those with unlimited geographical scope, such as medical and emergency relief charities. If they have a defined area of benefit, charities are only able to expend their funds within that defined area. If this area is an overseas country or jurisdiction, the charity can quite properly be transferring funds to that country

or jurisdiction. It would otherwise be less clear why the organisation should be transferring funds to a third country (which may, within the general context of the banks risk assessment have a lower profile) and this would therefore be unusual. Such activity would lead to the charity being regarded as higher risk.

FATF Recommendations 8

2.5.77 Non-profit organisations are suitable vehicles for TF for terrorists and terrorist organisations. The risks relate to a possible dubious source of income/capital and cash donations, possible unclear (illegal) expenditures, possible TF and in a broader sense possible reputation risk for banks. Charitable organisations may have a CBF (Central Bureau for Fundraising) quality mark and/or an ANBI status or registration this does not guarantee that the risk is mitigated related to the integrity of the NPO. Organisations without a quality mark or registration (such as CBF or ANBI) may also lack transparency or supervision. As a result, these organisations may pose a higher risk to banks.

2.5.78 In the past non-profit organisations have been abused in diverting funds to TF and other criminal activities. FATF published a best practices paper on 'Combating the abuse of non-profit organisations' in June 2015 (available at www.fatf-gafi.org), in support of Recommendation 8. In November 2005, the European Commission adopted a Recommendation to member states containing a Framework for a code of conduct for non-profit organisations.

2.5.79 Whilst banks may conclude on the basis of their due diligence that the request for facilities is acceptable, they should bear in mind that terms like 'foundation', 'stiftung', 'anstalt' are liable to be hijacked by prime bank instrument fraudsters to add spurious credibility to bogus investment schemes.

Associations

2.5.80 There are essentially two types of associations ("vereniging"):

1. Association with legal personality: the association has the full legal capacity ("volledige rechtsbevoegdheid"), in theory there is no personal liability for its obligations. Just as with a foundation a civil-law notary is needed to draft a deed, stating that the foundation has been established and listing its statutes. It is mandatory to register an association with "full legal capacity" at the trade register

of the Chamber of Commerce. An association with full legal capacity" has the same rights and duties as a natural person. For example, it can take out loans and own and inherit registered property. Subsidy providers often require that associations have "full legal capacity".

2. Association with limited legal capacity ("vereniging met beperkte rechtsbevoegdheid"). Such an association can be established without a notarial deed. In that case the informal association will only have "limited legal capacity" ("beperkte rechtsbevoegdheid"). The officers of an informal association will be held personally liable for its obligations. This liability can be limited by entering the association in the trade register of the Chamber of Commercial. An association with "limited legal capacity" cannot own a registered property, e.g. real estate.

Mutual benefit associations

2.5.81 The mutual insurance company (onderlinge waarborgmaatschappij) is a cooperative in which the members enter into insurance agreements with each other and the company, so that all members can profit from the agreements.

Cooperatives

2.5.82 A cooperative is a special type of association that enters into specific agreements with and on behalf of its members. Two common forms are the "business cooperative" ("bedrijfscoöperatie") and the "entrepreneurs cooperative" ("ondernemerscoöperatie").

- A business cooperative supports the business interests of its members in certain areas, e.g. procurement or advertising. A well-known example of a business cooperative in the Netherlands is FrieslandCampina, a large dairy cooperative whose members are dairy farmers who share in the cooperative's profits;
- The members of an "entrepreneurs cooperative" work independently, but can also join forces to take on certain projects.

Members have voting rights and can enter or leave without jeopardising the cooperative's continued existence. An entrepreneurs' cooperative is ideal for small-scale and/or short-term collaborative ventures.

2.5.83 The cooperative assumes liability as a legal entity. When the cooperative is dissolved and its outstanding debts need to be resolved, the members are liable for an equal share. However, it is possible to exclude liability by setting up a “cooperative with limited liability” (“coöperatie met beperkte aansprakelijkheid, BA”) or a “cooperative with excluded liability” (“coöperatie met uitgesloten aansprakelijkheidcooperative, UA”).

Partnerships

2.5.84 A partnership can be described as a community of persons created by an agreement. A partnership is not a legal person and is therefore not the person with whom a customer relationship is established or for whom a transaction is carried out. There are general partnerships, limited partnerships, or similar communities of unincorporated persons or similar entities governed by foreign law. A general partnership may for instance consist of natural and/or legal persons who together constitute the company that is the customer of the bank.

Wwft 1(1)

2.5.85 Under the terms of the Wwft, only a natural person or a legal entity can be a ‘customer’; a partnership (partnership, general partnership, limited partnership) as such can therefore not be a customer. In principle, the Wwft assumes that the individual partners (natural persons or legal entities) should be regarded as customers. Partnerships are different from private individuals in that there is an underlying business. This business is likely to have a different ML/TF risk profile from that of an individual.

2.5.89 Given the wide range of unincorporated businesses, in terms of size, reputation and numbers of partners/principals, banks may consider making an assessment of where a particular partnership or business lies on the associated risk spectrum.

2.5.87 It is the bank’s obligation to verify the identity of the customer using evidence from a reliable source, independent of the customer. Where unincorporated businesses are well-known, reputable organizations, with long histories in their industries, and with substantial public information about them and their principals and controllers, confirmation of the customer’s membership of a relevant professional or trade association can likely provide such

reliable and independent evidence. This does not obviate the need to verify the identity of the partnership's beneficial owners.

2.5.88 Other partnerships will have a lower profile, and will generally comprise a much smaller number of partners/principals. When verifying the identity of such customers, banks should primarily consider the number of partner/principals. Where these are relatively few, the customer should be treated as a collection of private individuals, and follow the guidance set out in 2.4; where numbers are larger, the bank can decide whether it could continue to regard the customer as a collection of private individuals, or whether it can be satisfied with evidence of membership of a relevant professional or trade association. In either circumstance, it is probably necessary to see the partnership so as to be satisfied that the entity exists, unless an entry in an appropriate national register may be checked. "Vennootschappen onder firma (VOF)" and "commanditaire vennootschappen (CV)" must be registered in the trade register of the Chamber of Commerce. Additional information can be derived from the partnership agreement.

2.5.89 In relation to partnerships the UBO is defined as any natural person(s):

.

- With an interest of more than 25% in the assets of the partnership, if it were to be dissolved;
- Entitled to more than 25% of the profits of the partnership;
- Who, in decision making about amendments of the partnership agreement or the performance of the partnership agreement other than day-to-day management, has the ability to exercise more than 25% of the voting rights;
- Who has factual control over the partnership.

If no UBOs can be identified based on the above, all general partners must be classified as UBO (senior managing official(s)).

Limited partnership ("commanditaire vennootschap")

2.5.90 A limited partnership (CV) does not have legal personality. A CV is established by means of a partnership agreement and has managing and silent partners. A CV is registered in the Trade Register of the Chamber of Commerce.

2.5.91 Use of a CV entails opacity because the partnership agreement is not publicly available. As a result, the silent partners cannot be identified and verified on the basis of public sources. Due to tax considerations , a CV is often used in real estate combinations and as an investment fund / investment vehicle. This may result in a combination of several ML/TF risks (e.g. complex ownership structures and / or legal form risks).

2.5.92 The managing partners are authorized to act on behalf of CV and are personally liable or jointly and severally liable for the debts of the CV. In the case of two or more managing partners, the absence of a written partnership agreement with third parties cannot serve as proof that no CV has been established. In addition, registration in the Trade Register of the Chamber of Commerce is required if the CV runs a business. CVs that do not run a business need not to be registered in the trade register of the Chamber of Commerce.

2.5.93 Silent partners, also called limited partners, only contribute financially to the limited partnership. They cannot act on behalf of the CV and have no direct influence on the partnership. The silent partners only contribute capital. They share the profits and their loss is limited to their contribution. When a silent partner starts acting on behalf of the CV the silent partner becomes jointly and severally liable (see paragraph 2.5.89).

Trust and equivalent legal arrangements

2.5.94 Under Dutch law, there is no trust or any other comparable legal arrangement that incorporates the legal effects mentioned below. The trust (under Anglo-American law) can be established without many formalities. They may be based on an express legal act but may also be instituted by operation of law. A trust may have various forms. It is not a legal person according to Dutch law. Most trusts are not separate legal persons, and for AML/CTF purposes they should be identified as described in paragraphs below.

2.5.95 The legal relationships created - inter vivos or on death - by a person, the settlor, when assets have been placed under the control of a trustee for the benefit of a beneficiary or for a specified purpose. In some cases the settlor has appointed a protector or controller who can remove the trustee in case of misconduct and in some cases even appoint a new trustee.

2.5.96 A trust has the following characteristics:

- The assets constitute a separate fund and are not a part of the trustee's own estate;
- Title to the trust assets stands in the name of the trustee or in the name of another person on behalf of the trustee;
- The trustee has the power and the duty, in respect of which he is accountable, to manage, employ or dispose of the assets in accordance with the terms of the trust and the special duties imposed upon him by law.

The reservation by the settlor of certain rights and powers, and the fact that the trustee may himself have rights as a beneficiary, are not necessarily inconsistent with the existence of a trust.

2.5.97 There is a wide variety of trusts and legal arrangements (anstalt, fiducie, treuhand, fideicomiso (legal arrangement)). It is important, when putting proprtionate AML/CTF processes into place, and when carrying out risk assessments, that banks take account of the various ML/TF risks that trusts of different sizes, areas of activity and due to the nature of business conducted, present.

2.5.98 For trusts or similar legal arrangements that are no legal persons, those trustees (or equivalent) who enter into the customer relationship with the bank, in their capacity as trustees of the particular trust or similar legal arrangement, are the bank's customers on whom the bank must carry out their CDD measures. Following a risk-based approach, in the case of a large, well-known and accountable organisation banks may limit the trustees who are considered customers to those who give instructions to the bank. Other trustees will be verified as beneficial owners.

2.5.99 For trusts and other equivalent legal arrangements that administer and distribute funds, the UBO is defined to at least include the following:

- The settlor(s);
- The trustee(s);
- The protector(s) if any;
- The beneficiaries or in case the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up of operates and

- Any other natural person exercising ultimate control over the trust by means of direct or indirect ownership of by other means.

2.5.100 In some trusts and similar arrangements, instead of being an individual, the beneficial owner may be a class of persons who may benefit from the trust. Where only a class of persons is required to be identified, it is sufficient for the bank to ascertain and name the scope of the class. It is not necessary to identify every individual member of the class. The information obtained should nevertheless be sufficient for the bank to establish at the time of payment the identity of the UBO.

2.5.101 Other “equivalent legal arrangements” should be understood to encompass any entities other than natural persons that can establish a permanent customer relationship with the bank or otherwise own property. This can include anstalt, fiducie, treuhand, fideicomiso and other relevant similar entities.

2.5.102 In exceptional cases where persons other than trustees, the settlor and beneficiaries exercise control over the trust property, they are to be considered as beneficial owners. Examples of such persons may include trust protectors.

2.5.103 For the vast majority of relevant trusts, either there will be clearly identified beneficiaries (who are beneficial owners within the meaning of the Wwft) or a class of beneficiaries. These persons will be self-evident from a review of the trust’s constitution.

Wwft 33

2.5.104 In respect of trusts, the banks should obtain the following information:

- Name of the settlor;
- Full name of the trust;
- Nature, purpose and objects of the trust (e.g., discretionary, testamentary, bare);
- Country of establishment;
- Names of all trustees;
- Names of any beneficiaries (or, when relevant and as set out in paragraph 2.5.103, a description of the class of beneficiaries);
- Name of any protector or controller;
- The purpose and nature of the trust or other legal arrangement;
- The law governing the trust or other legal arrangement.

2.5.105 The identity of the trust must be verified on the basis of documents, data or information obtained from a reliable source that is independent of the customer. This may require insight into relevant extracts from the trust deed (the agreement on which the trust is based and by which the trust is managed), or reference to an appropriate register in the country of establishment. The bank must take reasonable measures to understand the ownership and control structure of the customer.

2.5.106 Where a trustee is itself a regulated entity (or a nominee company owned and controlled by a regulated entity), or a company listed on a Recognised Exchange, or other type of entity, the identification and verification procedures that should be carried out should reflect the standard approach for such an entity.

2.5.107 Banks may consider distinguishing between those trusts that serve a limited purpose (such as inheritance tax planning) or have a limited range of activities and those where the activities and connections are more sophisticated, or are geographically based in and/or have financial links to other countries.

2.5.108 For situations presenting a lower ML/TF risk, standard evidence will be sufficient. However, less transparent and more complex structures, with numerous layers, may pose a higher ML/TF risk. Some trusts established in jurisdictions with favourable tax regimes were in the past associated with tax evasion and ML/TF. In respect of trusts in this category, the bank's risk assessment may lead to requiring additional information on the purpose, funding and beneficiaries of the trust.

2.5.109 Where a situation is assessed as carrying a higher risk of ML/TF , the bank may consider carrying out a higher level of verification. Information that might be appropriate to ascertain for higher risk situations includes:

- Donor/settlor/grantor of the funds (except where there are large numbers of small donors);
- Domicile of business/activity;
- Nature of business/activity;
- Location of business/activity (operating address).

Trust and Company Service Providers (TCSPs)

SW 1977

2.5.110 TCSPs are financial service providers that facilitate businesses by providing one or more entities with a physical domicile address, in combination with the performance of management, administration and management of tasks. The integrity supervision of the TCSPs in the Netherlands is based on the Trust Offices Supervision Act (Wtt), the Money Laundering and Terrorist Financing Prevention Act (Wwft) and the Sanction law (SW) 1977. TCSPs can only provide trust services in the Netherlands if they are licensed and supervised by DNB.

Wtt 1(a)

2.5.111 The Wtt describes trust services as follows: "A legal person, company or natural person who, whether or not jointly with other legal persons, companies or natural persons, provides one or [trust services] professionally or professionally."

Any natural or legal person that by way of business provides any of the following services to third parties:

- Forming companies or other legal persons;
- Acting as, or arranging for another person to act as, a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- Providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement;
- Acting as, or arranging for another person to act as, a trustee of an express trust or a similar legal arrangement;
- Acting as, or arranging for another person to act as, a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements in accordance with EU law or subject to equivalent international standards.

Foreign legal entities

2.5.112 Foreign legal forms may deviate in their transparency, liability and obligations from the laws and regulations that apply to Dutch legal forms. Local laws and regulations relating to the integrity of business operations or, more specifically, to the prevention of ML/TF may vary considerably from jurisdiction to jurisdiction. Foreign legal forms established in the Netherlands are subject to

Dutch law. In addition, a foreign company with an office in the Netherlands must be registered in the Dutch Trade Register.

2.5.113 If the legal form does not fall under one of the forms described in section 2.5, it must be a foreign legal form. Just as in the Netherlands, there are many different legal forms abroad that vary per country. In order to determine the UBOs and other parties involved with the customer, it is necessary to request the correct information from the customer. This is why it is important to have a good understanding of the legal form of the customer. Therefore, banks may consider assessing at all times the characteristics of the legal form in question (for example whether it its capital is divided into shares, the entity has capital, there are partners, there may be a silent partner, etc.)

Wwft 11(2)(3)

2.5.114 If the client is a foreign legal entity that is not established in the Netherlands, the identity will be verified on the basis of:

- Reliable and in the international course of business commonly used documents, data or information from an independent source;
- Documents, data or information recognized by law as a valid means of identification in the customer's state of origin.

2.5.115 For foreign legal forms, extra attention should be paid to:

- For what reason the entity would like to open the account in the Netherlands e.g. background checks, legal structure.
- The extent to which the legal form deviates in terms of transparency, liability and obligations from the laws and regulations that apply to Dutch legal forms (for example, a legal form that allows anonymous shareholders);
- If the entity is established in a country other than the country under whose law it is incorporated, the reason why a foreign legal form is used (is it plausibly a branch or is there another reason);
- The country-specific method of identification and verification of the customer and parties involved with the customer that deviates from Dutch laws and regulations on identification and verification (for example, a method of identification and/or verification that is less strict in the country of the legal form than in the Netherlands).

2.6 Multipartite relationships, including reliance on third parties

2.6.1 Frequently, a customer may have contact with two or more institutions (see 2.6.6) in respect of the same transaction. This can be the case in both the retail market, where customers are routinely introduced by one institution to another, or deal with one institution through another, and in some wholesale markets, such as syndicated lending, where several institutions may participate in a single loan to a customer.

2.6.2 However, several institutions requesting the same information from the same customer in respect of the same transaction does not only not help in the fight against financial crime, but also adds to the inconvenience for the customer. It is important, therefore, that in all circumstances each institution is clear as to its relationship with the customer and its related AML/CTF obligations, and as to the extent to which it can rely upon or otherwise take account of the verification of the customer that another institution has carried out. Such account must be taken in a balanced way that appropriately reflects the ML/TF risks. Account must also be taken of the fact that some of the institutions involved may not be NL-based.

2.6.3 In other cases, a customer may be an existing customer of another regulated institution in the same group. Guidance on meeting AML/CTF obligations in such a relationship is given in paragraphs 2.6.14 – 2.6.15.

Reliance on third parties

Wwft 3(2)(d),5(1)(a), (b)

2.6.4 The Wwft expressly permits an institution to rely on another institution to apply any or all of the CDD measures, provided that the other institution is listed in article 5 (1)(a) Wwft (see paragraph 2.6.6). The relying institution (bank), however, retains responsibility for any failure to comply with a requirement of the Wwft, as this responsibility cannot be delegated. Furthermore, it is not allowed to place reliance on a third party for the ongoing monitoring obligation on the customer relationship.

2.6.5 For example:

- Where an institution (institution A) enters into a customer relationship with, or undertakes an occasional transaction

for, the underlying customer of another institution (institution B), for example by accepting instructions from the customer (given through Institution B); or
- Institution A and institution B both act for the same customer in respect of a transaction (e.g., institution A as executing broker and institution B as clearing broker).

Institution A may rely on institution B to carry out CDD measures, while remaining ultimately liable for compliance with the Wwft.

Wwft 5 (1)(a)

2.6.6. In this context, institution B must be:

1. An institution mentioned in article 1a (4)(a), (b), (c), (d), (e) Wwft established in the NL or in another member state;
2. An institution mentioned in article 1a (4)(f) Wwft who has a license as referred to in article 2 (1) or (2) “Wet toezicht trustkantoren (wtt)”;
3. An institution as referred to in article 1a (2) and (3) Wwft or a branch of that institution established in the NL or in another member state;
4. An institution mentioned under (1) and (3) above who carries on business in a third country as designated by the Dutch Minister of Finance not being a member state and who is subject to, and supervised for compliance with, CDD and record keeping requirements equivalent to those laid down in Wwft. (Currently there are no countries designated by the minister).

It is prohibited to place reliance on third parties established in high-risk countries as designated by the EU Commission.

Wwft 5(1)(c)

2.6.7 Where a bank relies on a third party to carry out CDD measures, it must immediately obtain from the third party all the identification and verification information and other data regarding the identity of the customer, the beneficial owner and/or the authorised representative.

Wwft 5 (1)(c), section 4.2 DNB Guidance on the AML/CFT Act and the Sanctions Act

2.6.8 The bank must enter into arrangements with the institution being relied on which:

- Enable the bank to obtain from the third party immediately upon request copies of any identification and verification data and any other relevant documentation on the identity of the customer, the beneficial owner and/or the authorised representative. It is however recommended that the third party makes available copies of the data and documentation to the bank immediately on introduction;
- Require the third party to retain copies of the data and documents referred to for the periods set out in article 33 (3) Wwft if copies of the data and documents are not made available to the bank on introduction (see paragraphs 6.12 and 6.18).

Wwft 10

2.6.9 Nothing in the Wwft prevents a bank from applying CDD measures by means of an agent or an outsourcing service provider (but see paragraphs 2.6.11), as long as the arrangements between the bank and the agent or outsourcing service provider stipulate that the bank remains liable for any failure to apply such measures.

Basis of reliance

Section 4.2 DNB Guidance on the AML/CFT Act and the Sanctions Act

2.6.10 For one institution to rely on verification carried out by another institution, the verification that the institution being relied upon has carried out must have been based at least on the standard level of customer verification. It is not permissible to rely on a CDD-level appropriate for lower risk situations. If the institution being relied on has undertaken CDD for lower risk situations, the relying institution can ask the introducing institution for further identification and verification details or may decide to undertake CDD themselves.

2.6.11 Whether a bank wishes to place reliance on a third party will be part of the bank's risk-based assessment, which, in addition to coninstitutioning the third party's regulated status, may include consideration of matters such as:

- Its public disciplinary record, to the extent that this is available;
- The nature of the customer, the product/service sought and the sums involved;
- Any adverse experience of the other institution's general efficiency in business dealings;

- Any other knowledge, whether obtained at the outset of the relationship or subsequently, that the bank has regarding the standing of the institution to be relied upon;
- Relevant CDD requirements have been carried out in accordance with the Wwft (or equivalent legislation in international situations).

If a bank repeatedly accepts customers from the same other institution, it is logical that it requests and assesses the CDD procedures of that institution using a risk-based approach.

2.6.12 A bank must document the steps taken to coninstitution that the institution relied upon satisfies the requirements in Wwft article 5 (1)(a). This is particularly important where the institution relied upon is situated outside the EEA.

2.6.13 Part of the bank's AML/CTF policy statement should address the circumstances where reliance may be placed on other institutions and how the bank assesses whether the other institution satisfies the definition of third party in Wwft article 5 (1)(a)Wwft (see paragraph 2.6.6).

Groups introductions

Wwft 5 (1)(a)(5°), (2)

2.6.14 Where customers are introduced between different parts of the same financial sector group, entities that are part of the group should be able to rely on identification procedures conducted by that part of the group that first dealt with the customer provided that the entities within the group comply with a group-wide program imposing CDD measures and rules on record-keeping in accordance with Wwft, the Directive (EU) 2015/849 or equivalent AML/CTF standards. One member of a group should be able to coninstitution to another part of the group that the identity of the customer has been appropriately verified.

2.6.15 Where a customer is introduced by one part of a financial sector group to another, it is not necessary for his identity to be re-verified, provided that:

- The identity of the customer has been verified by the introducing part of the group in line with AML/CTF standards of the Wwft, the Directive (EU) 2015/849 or equivalent AML/CTF standards;

- The group entity that carried out the CDD measures can be relied upon as a third party under Wwft article 5 (1)(a); and
- The group to which this entity belongs is subject to a robust supervision for compliance with these CDD measures.

Branches and majority-owned subsidiaries of institutions established in the EU may be exempted from the prohibition that reliance cannot be placed on parties established in high-risk countries as designated by the EU Commission where those branches and majority-owned subsidiaries fully comply with the group-wide AML/TF program.

Situations which are not reliance

(i) One institution acting solely as introducer

2.6.16 At one end of the spectrum, one institution may act solely as an introducer between the customer and the bank providing the product or service and may have no further relationship with the customer. The introducer plays no part in the transaction between the customer and the bank and has no relationship with either of these parties that would constitute a customer relationship. This would be the case, for example, with respect to name-passing brokers in inter-professional markets.

2.6.17 In these circumstances, where the introducer neither gives advice nor plays any part in the negotiation or execution of the transaction, the identification and verification obligations under the Wwft lie with the product/service providing bank. This does not, of course, preclude the introducing institution carrying out identification and verification of the customer on behalf of the bank providing the product or service, as agent for that bank (see paragraphs 2.6.19 – 2.6.20).

(ii) Where the intermediary is the agent of the product/service provider

2.6.18 If the intermediary is an agent or appointed representative of the product or service providing bank, it is an extension of that bank. The intermediary may actually obtain the appropriate verification evidence in respect of the customer, but the product/service providing bank is responsible for specifying what must be obtained, and for ensuring that records of the appropriate

verification evidence taken in respect of the customer are retained.

2.6.19 Similarly, where the product/service providing bank has a direct sales force, they are part of the bank, whether or not they operate under a separate group legal entity. The bank is responsible for specifying what is required, and for ensuring that records of the appropriate verification evidence taken in respect of the customer are retained.

(iii) Where the intermediary is the agent of the customer

2.6.20 From the point of view of a product/service providing banker, the position of an intermediary, as agent of the customer, is influenced by a number of factors. The intermediary may be subject to the Wwft, or otherwise to the Directive (EU) 2015/849, or to similar legislation in an assessed low-risk jurisdiction. It may be regulated; it may be based in the Netherlands, elsewhere within the EU, or in a country or jurisdiction outside the EU, which may or may not be a FATF member. Guidance on assessing which countries or jurisdictions might be low-risk jurisdictions is given at Annex 1-I.

2.6.21 Depending on the jurisdiction, where the customer is an intermediary carrying on appropriately regulated business, and is acting on behalf of another, and the bank determines that the situation presents a low degree of risk of ML/TF, the product providing bank may decide to carry out CDD measures appropriate for lower risk situations on both the customer and on the underlying party.

2.6.22 Where a bank cannot apply a lower level of CDD requirements to the intermediary, the product/service providing bank is obliged to carry out CDD measures on the intermediary and, as the intermediary acts for another, on the underlying customer.

2.6.23 Where the bank takes instruction from the underlying customer, or where the bank acts on the underlying customer's behalf (e.g., as a custodian) the bank then has an obligation to carry out CDD measures in respect of that customer, although the reliance provisions may be applied.

2.6.24 In these circumstances, in verifying the identity of the underlying customer, the bank may take a risk-based approach. It will need to assess the AML/CTF regime in the intermediary's jurisdiction,

the level of reliance that can be placed on the intermediary and the verification work it has carried out, and as a consequence, the amount of evidence that should be obtained direct from the customer.

2.6.25 In particular, where the intermediary is located in a higher risk jurisdiction, or in a country listed as having material deficiencies, the risk-based approach must be aimed at ensuring that the business does not proceed unless the identity of the underlying customers has been verified to the product/service providing bank satisfaction.

2.7 Identification and verification by third parties (outsourcing /introduction)

Wwft 5(1)(a),10 (1)

2.7.1 Pursuant to the Wwft one may rely on a third party carrying out aspects of the customer due diligence. This is possible in the following situations:
- “Introduction” by another institution subject to Wwft regulation, which has already completed aspects of the customer due diligence.
- “Outsourcing” of the customer due diligence analysis as part of an outsourcing agreement or agency agreement.
Third parties on which reliance is placed should be subject to Wwft regulation.

DNB Guidance, Outsourcing chapter 4.8

2.7.2 Aspects of the customer due diligence that cannot be outsourced are risk assessment and ongoing monitoring of the customer relationship, except when a third party is a member of the same group.

Wwft 10(2) and DNB Guidance, Chapter 4.8

2.7.3 Banks must take the following into account when relying on an introducing party or when outsourcing aspects of customer due diligence:

- The bank is and will remain at all times responsible for identification and verification, even in the event of outsourcing or introduction;
- Outsourcing will not lead to any deterioration in the quality of the bank's own independent assessment. In other words, the bank may not become completely dependent on the introducting or outsourcing partner;

- The bank must have sufficient insight and assurance that the procedures, measures and expertise of the introducting or outsourcing partner meet the required standard. Only in this way the bank can assess whether they continue to meet the requirements set by the Wwft;
- The bank has a clear policy and procedures for structural introduction and outsourcing;
- The bank must document introduction or outsourcing arrangements when they are of a structural nature. The bank may consider drawing up standard outsourcing agreements for this purpose;
- The following elements may be considered when drawing up standardised outsourcing agreements:
  - The bank may at any time make changes to the way in which the third party carries out the activities;
  - The third party is under an obligation to enable the bank to comply with the law on a continous basis;
  - Arrangements on the mutual exchange of information, including arrangements on making information available requested by supervisors in the performance of their statutory duties;
  - That supervisors have the possibility to conduct or have conducted on-site investigations at the premises of the third party;
  - The manner in which the agreement is terminated.

2.8 Monitoring customer activity

The requirement to monitor customers' activities

Wwft 3(2)(d), Bpr Wft 14 (4)

2.8.1 Banks must conduct ongoing monitoring of the customer relationship with their customers. Ongoing monitoring of the customer relationships includes:

- Scrutiny of transactions undertaken throughout the course of the relationship (including where necessary, the source of funds) to ensure that the transactions are consistent with bank's knowledge of the customer, his business and risk profile;
- Ensuring that the documentation or information obtained for the purpose of applying CDD are kept up to date.

2.8.2 Monitoring customer activity helps to identify unusual activity. If unusual activities cannot be rationally explained, they may

involve ML/TF. Monitoring customer activity and transactions that take place throughout a relationship helps banks know their customers, assist them to assess risk and provides greater assurance that the bank is not being used for the purposes of financial crime.

Post event transaction monitoring

DNB Guidance, Post-event transaction monitoring process for banks chapter 5

2.8.3 The SIRA plays a central role in this process of managing risks adequately. This risk analysis at operational level, in which both the first-line and the second-line staff are involved, provides the basis for a bank's integrity policies that must be regularly reviewed, and must be translated into procedures and measures. The results of the SIRA must affect the entire organisation, and must also be reflected in the risk analyses at customer level. Therefore, banks translate the risk of ML/TF identified in the SIRA into risk mitigating actions like the transaction monitoring process.

DNB Guidance, Post-event transaction monitoring process for banks chapter 4 & DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act, pp. 32-35

2.8.4 In determining the risk profile of the customer and/or customer peer groups, banks also involve the expected transaction behavior of the customer or the peer group to which the customer belongs. Banks can categorize their customer relations according to peer groups. Peer groups can be defined on the basis of a number of customer characteristics, for example customer segment, sectors, country of incorporation, legal form, countries in which the customer is active, etcetera. By preparing a transaction profile in this way (through peer grouping) a bank can sufficiently monitor transactions conducted throughout the duration of the relationship to ensure they are consistent with knowledge of the customer and the risk profile. Depending on the risk, mass retail customers could be included in homogeneous peer groups. To effectively monitor customer behavior, expected transaction behavior is compared to the customers risk profile or to the transactional behavior of a customers' peer group. A customer stays within its peer group as long as the actual behavior is in line with the expected transaction profile as established by the systems and tooling used by the bank.

DNB Guidance, Post-event transaction monitoring process for banks chapter 3

2.8.5 Banks may follow a risk-based approach in monitoring customer activity and must have adequate policies for transaction monitoring and underlying procedures, processes and systems.

Decree on Prudential Rules for Financial Undertakings 14(4)

2.8.6 Banks must have (automated) transaction monitoring systems that may comprise a set of adequate business rules, scenarios and/or models to detect ML/TF risks. Banks test these systems periodically, both on technical aspects and effectiveness.

Wwft 16, Decree on Prudential Rules for Financial Undertakings 17 and 18

2.8.7 Banks must have adequate reporting and alert handling processes. Banks must further ensure that intended and executed unusual transactions[37] are reported to FIU-NL without delay and in line with reporting requirements. Banks should use a case management system so that all actions are recorded and in order to ensure reports are filed timely and correctly. Failing to report, either intentionally or unintentionally, a suspicious activity constitutes an economic crime punishable in accordance with the Dutch Economic Offences Act and / or similar local laws and regulations. If the relevant authorities identify failure to report, they can impose a sanction, penalty and / or fine if this amounts to a failure to comply with local laws and regulations.

Decree on Prudential Rules for Financial Undertakings 18

2.8.8 Banks must have structured their governance with regard to monitoring in such a way that there is clear segregation of duties and in line with the three lines of defence model.

The requirement to monitor customers' activities

Wwft 1, 2a, 3(1) and 3(2d)

2.8.9 Bank's must conduct ongoing monitoring of the customer relationship with their customers. Ongoing monitoring of a customer relationship includes:

- Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the

.....

[37] Under Dutch law, a bank must have processes, procedures and systems in place to detect unusual transactions or (patterns of) behaviour and/or activity. Likewise, these unusual transactions or (patterns of) behaviour and/or activity need to be reported to the FIU. In some other jurisdictions, the threshold for reporting obligations is not 'unusual', but 'suspicious'.

bank's knowledge of the customer, his business, its payment transactions and risk profile;
- Ensuring that the documents,data or information obtained for the purposes of applying CDD are kept up to date;
- In this regard, a bank pays particular attention to unusual transaction patterns and to transactions that by their nature involve a higher risk of ML/TF.

DNB Guidance, Post-event transaction monitoring process for banks chapter 4

2.8.10 Monitoring customer activity is aimed at identifying unusual activity. In order to understand what is unusual, banks first need to identify the customer transaction profile. In order to determine a transaction profile of a customer, an expectation is outlined on the basis of the expected transactions or the expected use of a customer account. A bank can also make use of peer grouping in establishing a transaction profile. By creating such a transaction profile, it is possible to monitor whether the transactions carried out during the term of the relationship correspond with the knowledge the bank has of the customer and his risk profile. A feasible transaction profile in any case meets the following criteria:

- Current: the transaction profile is up-to-date and has a date. All relevant changes to the profile are made promptly;
- Complete: it includes all account numbers and all relevant activities (such as websites used by the customer);
- Specific and substantiated: the suspect flows of funds are clearly described, including the expected amounts (in view of the type of customer) and the frequency of the payments (the number of orders the merchant's customers have placed). The (threshold) amounts indicated are well substantiated and can actually contribute to recognizing unusual transactions;
- Documented: the transaction profile is documented in the customer file.

If unusual activities cannot be rationally explained, they may involve ML/TF. Monitoring customer activity and transactions that take place throughout a relationship helps bank's know their customers, assist them to assess risk and provides greater assurance that the bank is not being used for the purposes of financial crime.

What is monitoring?

Wwft 15 and 16, Decree on Prudential Rules for Financial Undertakings 17 and 18, Implementing decree Wwft 4 and Annex indicator list

2.8.11 The essentials of any system of monitoring are that:

- It flags (patterns of) transactions and/or activities for further examination;
- These reports are reviewed promptly by the right person(s);
- Appropriate action is taken as soon as possible but in any case in a timely manner on the findings of any further examination;
- Supports the ability to report. Executed or proposed unusual transactions must be notified to FIU-NL without delay upon their unusual nature becoming known.

As a result there is an obligation to have specific procedures and operational processes in place to assess and process transaction alerts and to report unusual transactions. Transactions are deemed unusual if they meet the objective or subjective indicators mentioned in the appendix of the implementing order of the Wwft. In this list the indicators are subdivided per type of institution and in objective and subjective indicators.

Objective indicator
Objective indicators are situations that have been labeled as unusual in the indicator list. The customer, his / her behavior or the context is not decisive here, but only the hard facts of the transaction. In addition:

- Different objective indicators apply to each type of institution, based on the nature of the institution;
- One of the objective indicators that apply to all institutions are transactions that are reported to the police or the Public Prosecutor's Office in connection with ML/TF; after all, there is the assumption that these transactions may be related to ML/TF;
- Transactions involving an objective indicator are called 'evidently unusual transactions' and must therefore be reported to FIU-the Netherlands without delay.

Subjective indicator
A subjective indicator is a transaction in which the institution has reason to assume that it can relate to ML/TF. Furthermore:

- Not only the individual transaction is decisive, but also transaction patterns and (the behavior of) the customer;
- No limit has been set for the subjective indicator;

- Important is the opinion of the (employee (s)) regarding the unusual nature of the transaction.

DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act, pp. 32-35

2.8.12 Monitoring can be either:

- In real time, in that transactions and/or activities can be reviewed as they take place or are about to take place, or
- After the event, through some independent review of the transactions and/or activities that a customer has undertaken

and in either case, unusual transactions or activities will be flagged for further examination.

DNB Guidance, Post-event transaction monitoring process for banks chapter 5.3

2.8.13 Monitoring may be by reference to specific types of transactions, to the profile of the customer, or by comparing their activity or profile with that of a similar, peer group of customers, or through a combination of these approaches.

DNB Guidance, Post-event transaction monitoring process for banks chapter 5.3, p. 23

2.8.14 Banks should also have systems and procedures to deal with customers who have not had contact with the bank for some time, in circumstances where regular contact might be expected, and with dormant accounts or relationships, to be able to identify future reactivation and unauthorized use.

2.8.15 In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer and product risk.

2.8.16 Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. The scope and complexity of the process will be influenced by the business activities, and whether the bank is large or small. The key elements of any system are having up-to-date customer information, on the basis of which it will be possible to spot the unusual, and asking pertinent questions to elicit the reasons for unusual transactions or activities in order to judge whether they may represent anything suspicious.

Nature of monitoring

2.8.17 Some financial services business typically involves transactions with customers about whom the bank has a good deal of information, acquired for both business and regulatory reasons. Other types of financial services business involve transactions with customers about whom the bank may need to have only limited information. The nature of the monitoring in any given case will therefore depend on the nature, size and business of the bank, the frequency of customer activity, and the types of customers that are involved.

Wwft 8

2.8.18 Higher risk accounts and customer relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring.

Manual or automated?

2.8.19 A monitoring system may be manual, or may be automated to the extent that a standard suite of exception reports are produced. One or other of these approaches may suit most banks. In the relatively few banks where there are major issues of volume, or where there are other factors that make a basic exception report regime inappropriate, a more sophisticated automated system may be necessary.

2.8.20 It is essential to recognize the importance of staff alertness. Such factors as staff intuition, direct exposure to a customer face to face or on the telephone, and the ability, through practical experience, to recognize transactions that do not seem to make sense for that customer, cannot be automated.

Wwft 16, Decree on Prudential Rules for Financial Undertakings 17 and 18

2.8.21 In relation to a bank's monitoring needs, an automated system may add value to manual systems and controls, provided that the parameters determining the results of the system are appropriate. Banks must understand the workings and rationale of an automated system, and must understand the reasons for its output of alerts, as it may be asked to explain this to its regulator.

2.8.22 There are many automated transaction monitoring systems available on the market; they use a variety of techniques to detect and report unusual/uncharacteristic activity. These techniques can range from artificial intelligence to simple rules.

The systems available are not designed to detect ML/TF, but are able to detect and report unusual/uncharacteristic behavior by customers, and patterns of behavior that are characteristic of ML/TF, which after analysis may lead to suspicion of ML/TF. The implementation of transaction monitoring systems is difficult due to the complexity of the underlying analytics used and their heavy reliance on customer reference data and transaction data.

2.8.23 Monitoring systems, manual or automated, can vary considerably in their approach to detecting and reporting unusual or uncharacteristic behavior. It is important for banks to ask questions of the supplier of an automated system, and internally within the business, whether in support of a manual or an automated system, to aid them in selecting a solution that meets their particular business needs best. Questions that must be addressed include:

- How does the solution enable the bank to implement a risk-based approach to customers, third parties and transactions?
- How do system parameters aid the risk-based approach and consequently affect the quality and volume of transactions alerted?
- What are the ML/TF typologies that the system addresses, and which component of the system addresses each typology? Are the typologies that are included with the system complete? Are they relevant to the bank's particular line of business?
- What functionality does the system provide to implement new typologies, how quickly can relevant new typologies be commissioned in the system and how can their validity be tested prior to activation in the live system?
- What functionality exists to provide the user with the reason that a transaction is alerted and is full evidence given for the reason?

2.8.24 What constitutes unusual or uncharacteristic behavior by a customer, is often defined by the system. It is important that the selected system has an appropriate definition of 'unusual or uncharacteristic' that is in line with the nature of business conducted by the bank.

2.8.25 The effectiveness of a monitoring system, automated or manual, in identifying unusual activity will depend on the quality of the parameters that determine what alerts it makes, and the ability of staff to assess and act as appropriate on these outputs. The

needs of each bank will therefore be different, and each system will vary in its capabilities according to the scale, nature and complexity of the business. It is important that the balance is right in setting the level at which an alert is generated; it is not enough to fix it so that the system generates just enough output for the existing staff complement to deal with – but equally, the system must not generate large numbers of 'false positives', which require excessive resources to investigate.

Alert handling

Wwft 16

2.8.26 Based on the expected transaction profile of a customer, banks must check and conclude on:

- Whether the actual transactions are consistent with that profile;
- Do the amounts involved match the expected transaction behavior;
- Does the frequency of the transactions reflect expected transaction behavior;
- Is the time frame for the transactions in line with the expected transaction behavior;
- Does the total volume of the transactions reflect expected transaction behavior;
- Is there a reasonable suspicion that the transaction(s) may be related to ML/TF;
- Is there a reasonable suspicion that the transaction(s) may be related to other types of crime, such as tax evasion; and
- Will this alert be escalated and subsequently reported as an unusual transaction?

Intended and executed transactions must be reported without delay after the unusual nature has been determined. In the event of a report, the bank provides the following information:

- The identity of the customer, the identity of the UBO's and, in sofar as possible, the identity of the person on whose behalf the transaction is executed;
- The nature and number of the identity document of the customer and, in sofar as possible, of the other persons referred to above;
- The nature, time and place of the transaction;
- The size and the destination and origin of the monies, securities, precious metals or other values involved in the transaction;

- The circumstances on the basis of which the transaction is considered unusual; and
- A description of the relevant items of great value in a transaction in excess of € 15,000.

CDD reviews

2.8.27 According to different legal and regulatory requirements, banks must carry out a review of the customers' due diligence files. This can be performed at different moments within the customer life cycle, by bank and/or customer driven events, during the execution of reviewing it is examined whether the customer still matches his/her risk profile and whether the transaction pattern is in line with expectations.

Wwft 3 (5), Directive (EU) 2015/849 11

2.8.28 In all cases a review of the customer file must take place. This means that even when there are no events a review on the customer file must still be performed. In this case there is always a time driven review in place (see paragraph 2.8.41).

Wwft 3 (5), Directive (EU) 2015/849 11

2.8.29 Continuous monitoring of the customer relationship and the transactions carried out during the course of this relationship must be performed, in order to ensure that these correspond to the bank's knowledge of the customer and his risk profile, including, if necessary, an examination of the source of the resources used in the customer relationship or transaction.

DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act 2.1

2.8.30 The bank compiles a risk profile of the customer based on the performed CDD. This risk profile is dynamic and can thus change over time. A review serves to determine whether the customer still meets the defined risk profile. To that end, the bank periodically updates all customer data, including the customer's risk profile, contact information and UBO(s). The basic principle is that the frequency and depth of the review depend on the risks presented by the customer.

The scope and definition of CDD reviews

2.8.31 CDD review can be triggered by events or by time. Expiry of time is basically the last event that can trigger a review if no other events have occurred or have been detected during the

customer's life cycle. If prior to the scheduled CDD review date, changes to the customer's profile occur that could potentially result in a change in customer risk classification a CDD review needs to be performed.

2.8.32 An event in this context is defined as a change in the customer data or circumstances that apply to a customer and/or customer group and that could potentially result in a change in the risk that the customer poses to the bank. This means that the bank may have to review and assess the customer's risk classification in light of the event.

Wwft 38)

2.8.33 Events that can potentially trigger a CDD review can be categorized into:

(1) Bank-driven event (change in (interpretation of) regulatory requirements, policy, market developments, etc.). For example when the risk level of a country changes due to a new sanctions regime, which might have considerable implications, a bank can decide, taking a risk-based approach, to finalize all CDD reviews, for customers affected by this change, within a year;
(2) Customer-driven event (change in products, ownership and control structure, adverse media, PEP involvement, customer behaviour, etc.). This change needs to be processed into the CDD file as soon as possible.

2.8.34 A CDD review needs to be performed within a reasonable period of time following a risk-based approach. For a bank-driven event this means that based on the outcome of a risk assessment it needs to be determined how soon the review of the impacted customers/customer groups must be finalized. Customer-driven events need to be assessed as soon as possible to determine if a full, partial or no review on the CDD file needs to be done. If a full CDD review is performed ahead of the next scheduled periodic review this could lead to an extension in the scheduled review date.

Starting point of CDD reviews / guiding principle of CDD reviews

Event Assessment

2.8.35 The starting point is to assess whether the trigger constitutes an event that has not been identified yet. If the event has already been identified before and processed in the CDD file, no further

action is required. For example, customer screening results in a hit on the PEP list. When checking the CDD file, it appears that the PEP has already been identified in the past based on other tools or information. Then no further action is required. In case the event has not been processed before, a materiality assessment must be performed.

Materiality assessment

2.8.36 An event is material if the change can potentially impact the risk rating of the customer. The change is considered non-material if no risk drivers are affected. Note that some non-material changes can be the result of another, material, change. For example, a name change of a company can be the result of a take-over or change in business activities. This will have to be assessed using a risk-based approach. The outcome could be that only an administrative update is required. Therefore assessing this event as not being a material change does not result in a full CDD being performed and cannot lead to an extension of the scheduled review date.

Execution of the CDD Review

2.8.37 The outcome of the above assessment may result in one of the following ways to perform the CDD review:

(1) Administrative update – The review of the customer is limited to recording the event, provided that there are no indications that a partial or full review is to take place. For example, a change in director, customer name change, change of address of the customer (within the same country). The action only consists of recording the change, attaching the evidence to the CDD file and perform screening where applicable. The CDD review date remains the same.

(2) Partial CDD review – A targeted review on a potential red flag that was identified. If after further research the red flag can be mitigated then no full CDD review is required. This assessment is recorded in the CDD file. The CDD review date remains the same.

(3) Event Driven Review (EDR) - This means that the change is so material that a full review of the customer needs to take place, performing a full risk assessment. Completion of the CDD review will result in a new CDD review date, driven by the customer's risk classification.

Event Driven Review Triggers

DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act 4.1.6

2.8.38 As a minimum the following events need to be assessed for materiality and, if applicable, a review needs to be initiated (list is non exhaustive):

- Doubts about the truthfulness or adequacy of previously obtained customer identification data;
- Change in customer's name;
- Change in legal form;
- Change in legal standing (in good standing, insolvent, in liquidation, bankrupt, etc.);
- Change in country risk (country of domicile, operation or activity);
- Change in ownership, tax, and/or shareholder structure;
- Change in UBOs;
- Change of person(s) acting as authorised representative(s) of the customer (officers, directors, authorised representatives);
- Material change in business activities, type of business, customer segment;
- Change in regulatory status/listing details;
- Change in products or services used by the customer;
- Change in customer's source of funds or source of wealth;
- Change in transaction pattern (including change in volume of cross-border transactions);
- New material adverse media (e.g. prosecution of the customer or relevant persons related to the company) or new developments in known adverse media;
- Change regarding PEP involvement;
- Change on sanctions;
- True hits from transaction screening/filtering;
- Change in local laws, regulations and/or internal policies in relation to due diligence;
- Customer involvement in legal proceedings;
- Transaction monitoring results that remain suspicious after investigation including SAR filings;
- There are indications that the customer may be involved in ML ;
- There are indications that the customer may be involved in TF;

- There are indications that the customer may be involved in criminal activities;
- Relevant warrant received / Customers assets attached (legal term for freezing assets) by order of competent authority.

Scope and definition Periodic Reviews

DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act 4.2.1

2.8.39 The ML/TF risk of a customer can change, therefore it is necessary to carry out periodic reviews to determine that the information about the customer is current and changes are assessed. The bank needs to determine a clear review cycle for each risk category or type of customer, for example at least once a year for high-risk cases, at least once every two to five years for medium risk cases and every five years for low risk cases. During the periodic review it is required to check whether all relevant information and/or documentation still reflect the actual situation of the customer.

2.8.40 However, in case of mass retail customers, a periodic CDD review might not be required, if sufficient controls are in place to identify, assess and, where necessary, act upon any changes in the customer's risk profile (including the identification of any suspicious transactions). In these situations, even when no changes have occurred since the previous CDD, a (manual/automated) risk assessment can still be performed to ensure that the risk profile of the customer is up to date and in line with the bank's risk appetite.

.

2.8.41 After completion of the CDD for new customers, the minimum frequency of the CDD review is then determined (i.e. the next scheduled CDD review date). The CDD file includes the date that the last CDD review was performed, as well as the information obtained during the review and the renewed risk assessment. CDD review is completed before the review date. If this is not possible because the customer refuses to provide the required information, this can be a reason to terminate the customer relationship or to restrict the use of products or services by the customer.

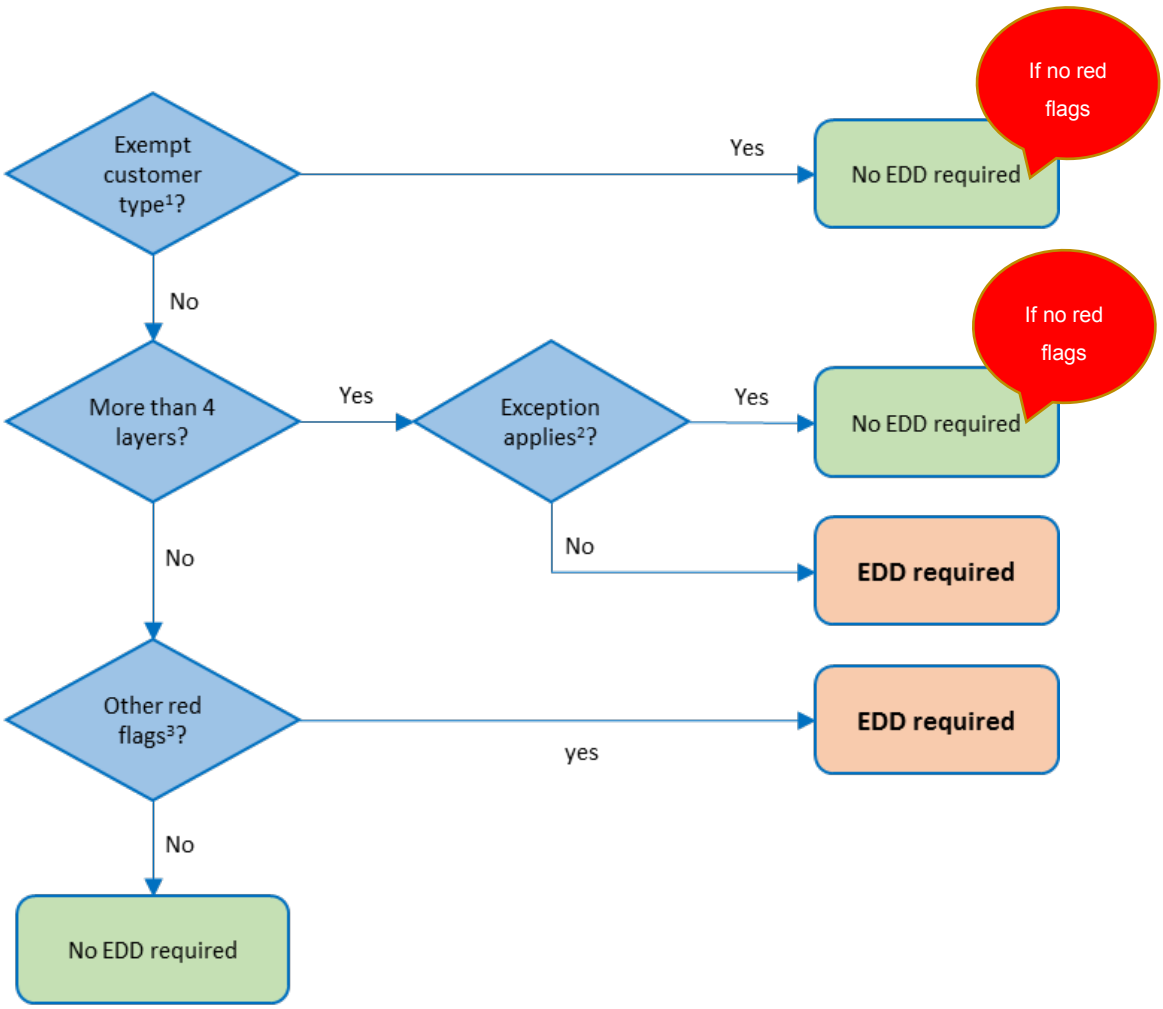
Annex 2-I Examples of supporting documents to evidence of funds/wealth

Categories	Possible details required	Possible verification documents
Savings from Employment Income	• Annual income and bonuses this year and last year • Nature of Employer's business • Employer's name/address	• Last 3 months' pay slips • Confirmation from employer of income and bonuses for last 2 years • Bank statements that clearly show receipt of the most recent 3 months' regular salary payments from the stated employer • Latest accounts if self-employed.
Maturing investments or encashment claim	• Amount received • From which company • Date received • How long held	• Letter/contract note from previous investment company giving notification of proceeds of maturing investment/claim
Share sale	• Sale value of shares sold • Description of shares/ funds • How sold (i.e. through stockbroker or bank etc.) and name/address • Date of sale • How long each investment held	• Legal sale document(s) (e.g. contract notes)
Property sale	• Sale value of property sold • Full address of property sold • How sold (i.e. through agent, by auction, private sale, including name/address) • Date of sale	• Signed letter from solicitor • Completed sale contract

	• How long property held	
Company sale or sale of an interest in company	• Name & address of company • Total sale price • Applicant's share • Nature of business • Date of sale	• Signed letter from solicitor • Signed letter from accountant • Copy of contract of sale • Sight of investment monies on bank statement
Inheritance	• Total amount received • Name of benefactor • Relationship to benefactor • Date received	• Grant of probate (with a copy of the will) which must include the value of the estate • Bank statements • Solicitor's letter
Loan	• Amount of loan • Why required • Name & address of Loan Provider • Date of loan	• Loan agreement • Recent loan statements
Gift	• Total amount • Details of benefactor • Reason for gift • Relationship to benefactor • Source of donated funds	• Letter from donor confirming details of gift and acknowledging the source of the donated funds • Based on the SOW specified, the donor might need to provide supporting documentation as per the provisions of this table
Company profits	• Copy of latest accounts • A letter from a regulated accountant giving details of company profits over the last 2 years	
Other income sources	• Nature of Income • Amount • Date Received • Received from whom	• Appropriate supporting documentation • Signed letter detailing funds from a regulated accountant

Annex 2-II Ownership and control structures

Decision tree EDD measures on complex structures



[1]Recognised Exchange Listed Entity, Equivalently Regulated Financial Institution, State-owned Enterprise, Privately-held Multinational
[2]All intermediate parents are in the same country as the customer, there are no other red flags in the structure and the structure fits the profile of the customer
[3]Presence of shell companies/offshore jurisdictions, bearer shares, trusts or similar legal arrangements, nominee shareholders and directors or the use of TCSPs in the set-up in the structure

Examples of situations where ownership does not equal control

1. Pyramidal ownership structures

A pyramidal ownership structure or ultimate majority control structure is defined as an entity whose ownership structure displays a top-down chain of control. In such a structure, the ultimate owners are located at the top and what follows below are successive layers of firms in which the parent company has a majority stake in the subsidiary. A direct result of this pyramidal ownership structure is a separation of actual ownership and control in firms located at the lower part of the pyramid structure. The separation of actual ownership and control occurs because the pyramid structure enables the ultimate beneficial owner to establish control disproportionately to the amount of ownership he has in every one of the successive firms. Pyramid structures are common in family businesses that try to attract outside investors while maintaining control. See example 1 below.

2. Different classes of shares

Most companies have only one class of shares, ordinary shares (also called common shares), but it is increasingly common for even very small private companies to have different share classes. This may be done for various reasons, such as to be able to vary the dividends paid to different shareholders, to create non-voting shares, shares for employees or family members, etc. A company can have whatever classes of shares it likes, and can call any class of shares by whatever name it chooses. Apart from ordinary shares, common types are preference shares, non-voting shares, A shares, B shares, etc. (sometimes called "alphabet shares"), shares with extra voting rights (sometimes called "management shares"). The share class system is infinitely flexible. Different classes of shares, and the rights attached to them, should be laid down in the company's articles of association.

3. Shareholders' Agreement

A shareholders' agreement is an agreement between the shareholders of a company. It can be between all or, in some cases, only some of the shareholders (such as, for instance, the holders of a particular class of share). Its purpose is to protect the shareholders' investment in the company, to establish a fair relationship between the shareholders and govern how the company is run.

The agreement will:

- Lay down the shareholders' rights and obligations;
- Stipulate which shareholders can appoint which executive and non-executive directors;
- Regulate the sale of shares in the company;
- Describe how the company is going to be run;
- Provide an element of protection for minority shareholders and the company; or

- Define how important decisions are to be made.

4. VIE structure

Another example of a contractual arrangement between shareholders is the so-called VIE structure. Variable Interest Entity (VIE) is a term used to refer to an entity (the investee) in which "the investor holds a controlling interest that is not based on the majority of voting rights." In China, foreign investors must obtain certain approvals from the government for their investments in China. It can be difficult to obtain approval to enter certain industries, especially restricted industries, such as telecommunication services, direct sales, mail order, and online sales. By using a VIE structure, foreign investors do not have to obtain PRC government approval for a foreign direct investment, since they do not own the equity of the operating company. However, they can still operate a domestic company and receive revenues from it. Examples of VIE structures are Baidu and Alibaba.

The simplest VIE structure includes a foreign customer, which is usually an exempt limited company in the Cayman Islands, a China wholly foreign-owned enterprise (WFOE) and a China domestic operating company owned only by Chinese nationals. The founders, foreign investors and other shareholders hold equity in the Caymans customer, which in turn owns a 100% equity interest in the WFOE.

The operating company is a purely China domestic company that is licensed to operate in the restricted industry in China. The key point of the VIE structure is that the WFOE exercises de facto control over the operating company through a series of contractual arrangements entered between the WFOE and the operating company. The Chinese founders of the domestic company borrow funds from the WFOE and pledge their shares in the operating company as collateral under the loan agreement.
See example 2 below.

5. Family-owned business

A family business is a commercial organisation in which ownership and/or control is in the hands of a family – related by blood or marriage or adoption. Family-owned businesses may have complex ownership and control structures for various reasons:

- To invite outside investors while at the same time retaining control over the family business;
- To protect the interests of the various family members and future generations;
- To allow easy transfer of ownership or profit rights to their children or other family members;
- To be able to separate control from profit interests as some family members may not be considered equally capable of running the family business;
- To shield the exact ownership and control relations within the family for privacy reasons.

The family members who are most influential, e.g. because they exert effective control over the main operating company or the ultimate parent, may be treated as UBOs.If no

single family member owns or controls more than 25% of the customer, then the ownership percentages of the individual family members should be combined, considering it as a family-controlled ownership interest.

Please note that shares can also be held by minors. In such case the voting rights will typically be exercised by a parent. Both may be considered UBOs.

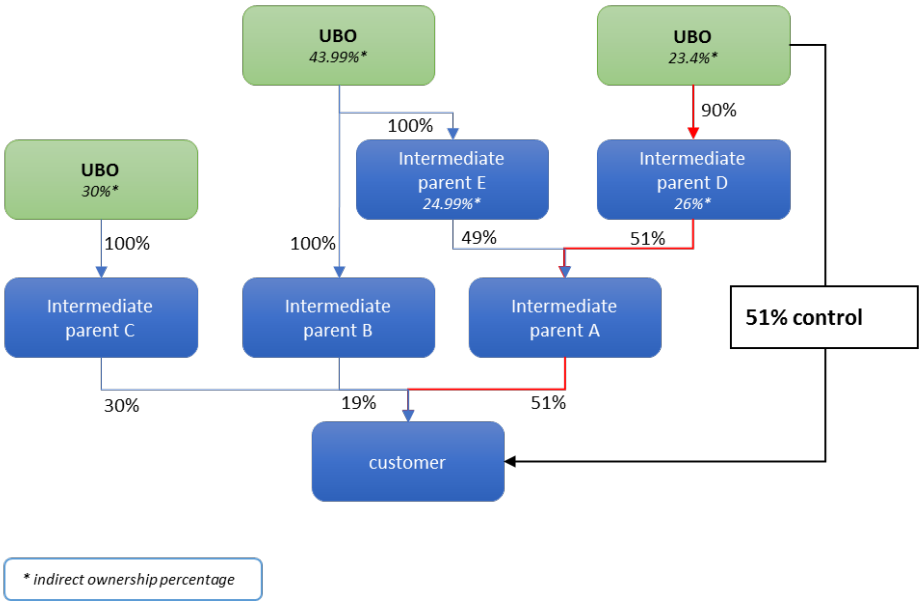
6. Usufruct
Usufruct (vruchtgebruik in Dutch) is a legal right in many civil law countries accorded to a person or party that confers the temporary right to use and derive income or benefit from someone else's property, e.g. shares. The owner (the “bare owner”) passes the voting and profit rights of his shares to another person (the “usufructuary”). Both the bare owner and the usufructuary have to be considered UBOs, as this is a kind of co-ownership.

7. Pledging
Similar to usufruct, shares can also be pledged, i.e. given as a security or collateral by the pledger to a pledgee. It can also mean that, depending on the pledge agreement, the voting and profits rights have been transferred to the pledgee.

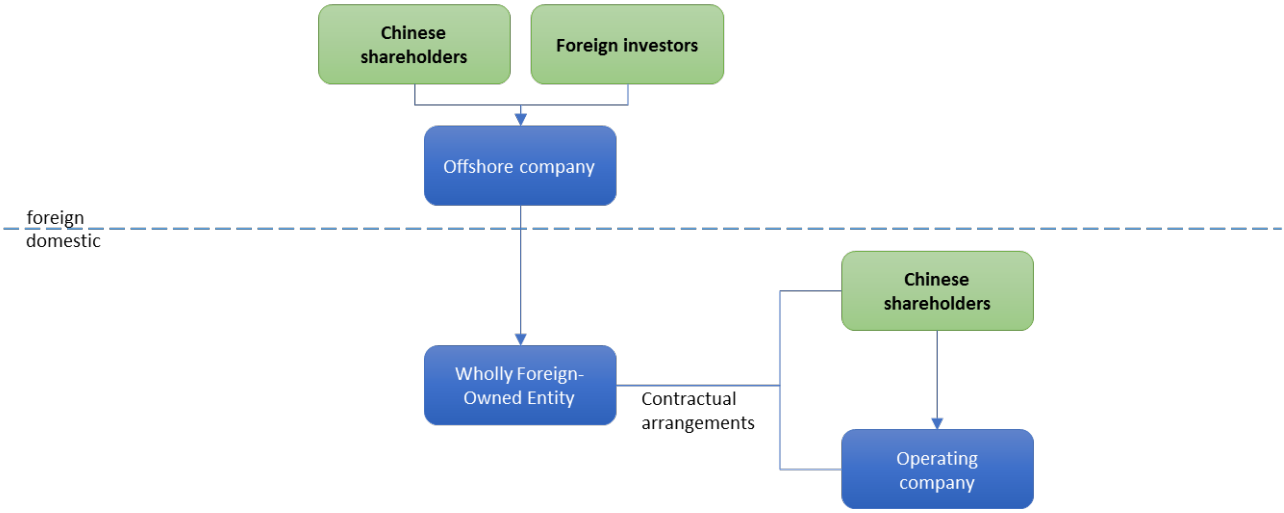
8. Parallel UBO structures
A customer can have multiple branches of ownership leading up to the same UBOs, while all direct and intermediate shareholdings stay below the thresholds of more than 25% that are generally stipulated by international AML/CTF legislation. For this reason it is important to have insight in the complete ownership and control structure in order to identify any cross-shareholdings.

Examples of complex structures

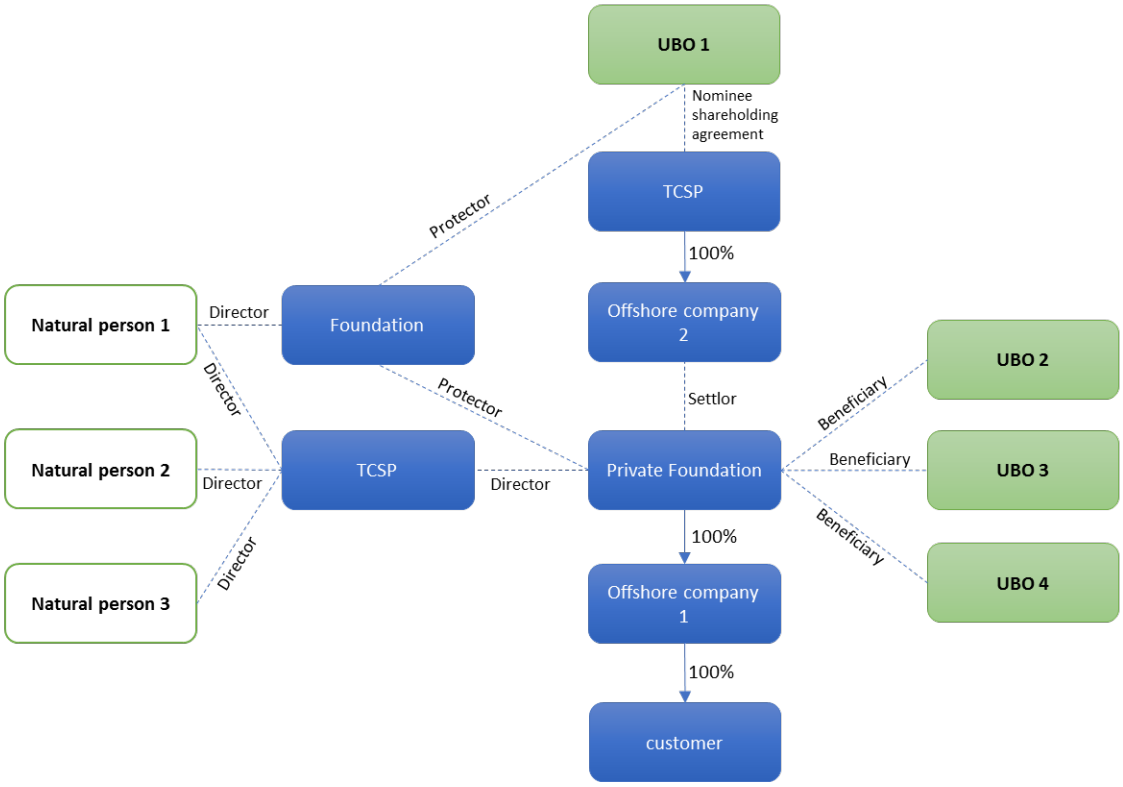
Example 1: Pyramidal Structure



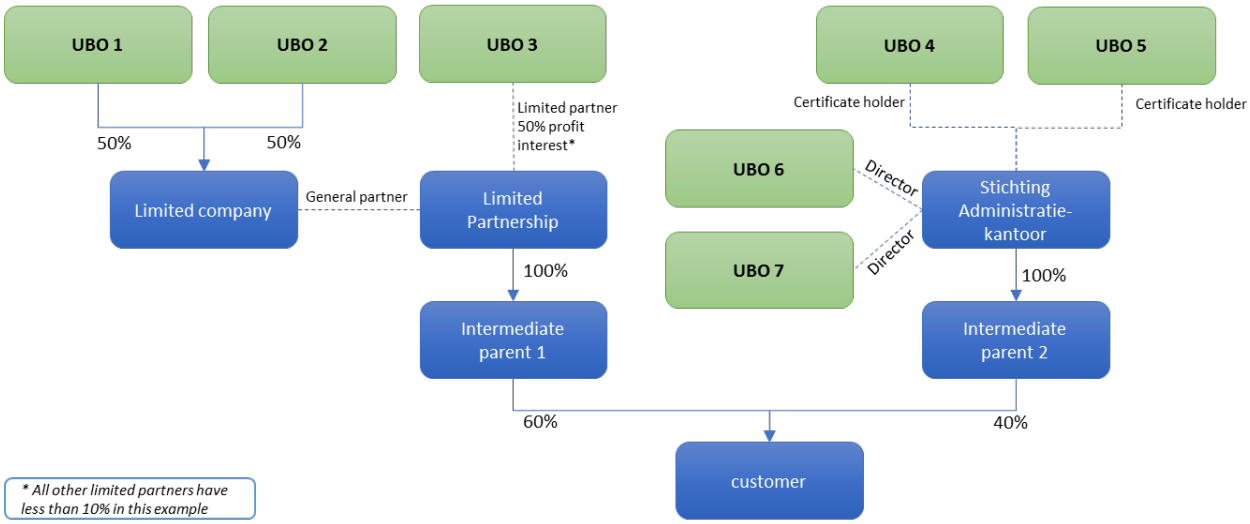
Example 2: VIE Structure



Example 3: Complex Entities Structure 1



Example 4: Complex Entities Structure 2



Chapter 3

Suspicious activities, reporting and data protection

3.1 Evaluation and determination by the nominated officer / identified staff

Regulation 21(5), Wwft 16

3.1.1 The bank's nominated officer must consider each report and determine whether it gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion. The bank must permit the nominated officer to have access to any information, including 'know your customer' information in the bank's possession, which could be relevant. The nominated officer may also require further information to be obtained, from the customer if necessary, or from an intermediary who introduced the customer to the bank, to the extent that the introducer still holds the information (bearing in mind his own record keeping requirements). Any approach to the customer or to the intermediary should be made sensitively, and probably by somebody else than the nominated officer, to minimize the risk of alerting the customer or an intermediary that a reporting to the FIU is be being considered.

3.1.2 In the appendix to Article 4 of the Wwft Implementation Decree 2018, objective and subjective indicators are specified for each type of institution based on which it must be assessed whether a transaction can or must be regarded as an unusual transaction.

3.1.3 As part of the review, other known connected accounts or relationships may need to be examined. Connectivity can arise commercially (through linked accounts, introducers, etc.), or through individuals (third parties, controllers, signatories etc.). Given the need for timely reporting, it may be prudent for the nominated officer to consider making a report to the FIU prior to completing a full review of linked or connected relationships, which may or may not subsequently need to be reported to the FIU.

3.1.4 If the nominated officer decides not to make a report to the FIU, the reasons for not doing so should be clearly documented, or recorded electronically, and retained with the internal suspicion report.

3.2 External reporting

Unusual transactions

Regulation 19(4)(d), Wwft 16t

3.2.1 The bank's nominated officer must report to the FIU any transaction or activity that, after his evaluation, he knows or suspects, or has reasonable grounds to know or suspect, may be linked to ML/TF, or to attempted ML/TF. Such reports of a completed or intended unusual transaction must take place immediately after the unusual nature of that transaction has become known.

A notification must also take place if the CDD has not provided the data prescribed by law, and there are also 'indications' that the client in question is involved in ML/TF. Even if an existing customer relationship is terminated because not all data prescribed by law are obtained and these 'indications' exist, a report must be made. In these cases, the report must also state why customer screening failed.

Wwft 16 (4)

3.2.2 An inherent part of the reporting duty is that institutions have in place processes and procedures to recognize and report the unusual nature of transactions. In addition, pursuant to Article 32 of the Wwft, the supervisory authorities may instruct an institution to develop internal procedures and controls to prevent ML/TF, if the institution fails to meet the requirement to report unusual transactions. There are also requirements based on other financial supervision legislation, which necessitate institutions to have procedures and measures in place to control integrity risks.

3.2.3 SARs are submitted electronically via a secure internet system.

3.2.4 In order to maintain an informed overview of the situation, all contact between departments/branches and law enforcement agencies should be controlled through, or reported back to a single contact point, which will typically be the nominated officer or identified staff. Alternatively, it may be appropriate to route

communications through an appropriate member of staff in the banks legal or compliance department.

3.2.5 A SAR's intelligence value is related to the quality of information it contains. A bank needs to have good base data from which to draw the information to be included in the SAR; there needs to be a system to enable the relevant information to be produced in hard copy for the law enforcement agencies, if requested under a court order.

Wwft 16,

3.2.6 Banks must include in each SAR all relevant information about the customer, transaction or activity that it has in its records.

Pursuant to Article 16 Wwft, in the event of a report, the bank provides the following:

- The identity of the customer, the identity of the UBO's and, to the extent possible, the identity of the person on whose behalf the transaction is executed;
- The nature and number of the identity document of the customer and, as far as possible, of the other persons referred to above;
- The nature, time and place of the transaction(s);
- The size, destination and/or origin of the monies, securities, precious metals or other values involved in the transactions;
- The circumstances based on which the transaction is considered unusual; and
- A description of the relevant items of great value in a transaction in excess of € 15,000.

Indentification

3.2.7 Article 19 of the Wwft provides for criminal indemnification and article 20 for civil indemnification. Criminal indemnification ensures that data or information provided by a bank that reports an unusual transaction in good faith cannot be used in a criminal investigation or prosecution of that bank on suspicion of ML/TF. The Act extends this indemnification to those who have submitted the report, such as a bank employee who submitted or helped compile the report.

Wwft 19, 20

3.2.8 Civil indemnification means that a bank cannot be held liable under civil law for the loss suffered by another party (the customer or a third party) as a result of a report if the bank acted on the reasonable assumption that it was implementing its reporting duty. For instance, claims in civil proceedings could be brought for breach of contract if the bank decided not to carry out a transaction but to report it. Legal action over an unlawful act is also possible, to claim alleged loss suffered as a result of a bank's unusual transaction report.

3.2.9 The indemnification will of course only apply if the unusual transaction report has been correctly submitted in good faith and in accordance with the requirements of the Wwft.

Confidentiality in case of SAR filing

Wwft 23

3.2.10 The Wwft imposes a strict duty of confidentiality. This means that banks are obliged to observe confidentiality with respect to an unusual transaction report. Exceptions are possible in sofar they arise from the law. Put briefly, these exceptions to the obligation of confidentiality allow the bank to exchange information with units of its own organization or network elsewhere (on a need to know basis) and/or other institutions that fall within the scope of the Wwft or equivalent legislation, within the framework of said laws. Without these exceptions, existing early-warning systems between banks, such as the interbank warning system, could be obstructed.

3.3 Data Protection - Subject Access Requests, where a unusual report has been made

Wwft 22

3.3.1 Occasionally, a Subject Access Request under the General Data Protection Regulation (GDPR) will include within its scope one or more SARs, which have been submitted in relation to that customer. It might be instinctively assumed that, to avoid tipping off, this kind of information should never be included when responding to the customer. However, an automatic assumption to that effect must not be made, even though in practice it will only rarely be decided that it is appropriate to include this information. Therefore, all such requests should be carefully considered on their merits in line with the principles below.

3.3.2 When making a request in writing (a Subject Access Request) to a data controller (i.e. any organization that holds personal data), an individual is normally entitled to:

- Be informed whether the data controller is processing (which includes merely holding) his personal data; and if so
- Be given a description of that data, the purposes for which they are being processed and to whom they are or may be disclosed; and
- Have communicated to him in an intelligible form all the information that constitutes his personal data and any information available to the data controller as to the source of that data.

GDPR 23, UAVG 41

3.3.3 Article 23 GDPR and article 41 UAVG provide that personal data are exempt from disclosure in any case where the application of that provision would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. However, even when relying on an exemption, data controllers (i.e. banks) should provide as much information as they can in response to a Subject Access Request.

3.3.4 Where a bank withholds a piece of information in reliance on article 41 UAVG exemption, it is not obliged to tell the individual that any information has been withheld. The information in question can simply be omitted and no reference made to it when responding to the individual who has made the request.

Wwft 22

3.3.5 Each Subject Access Request must be considered on its own merits in determining whether, in a case, the disclosure of an unusual transaction is likely to prejudice an investigation and, consequently, constitute a tipping-off offence. In determining whether the article 41 UAVG exemption applies, it is legitimate to take account of the fact that although the disclosure does not, in itself, provide clear evidence of criminal conduct when viewed in isolation, it might ultimately form part of a larger jigsaw of evidence in relation to a particular crime. It is also legitimate to take account generally of the confidential nature of unusual activity reports when considering whether the exemption under article 41 UAVG might apply.

3.3.6 Whenever disclosure has been made in legal proceedings or in a investigation and the full contents of such a disclosure has

already been revealed, it is less likely that the exemption under article 41 UAVG would apply. However, caution should be exercised when considering disclosures that have been made in legal proceedings for the purposes of the article 41 UAVG exemption, as often the disclosure will have been limited strictly to matters relevant to those proceedings, and other information contained in the original report may not have been revealed.

Wwft 22

3.3.7 In order to guard against a tipping-off offence, nominated officers must ensure that no information relating to SARs is released to any person without the nominated officer's authorization. Further consideration may need to be given to unusual transaction reports received internally that have not been submitted to the FIU. A record should be kept of the steps that have been taken in determining whether disclosure of a report would involve tipping off and/or the availability of the article 41 UAVG exemption.

Chapter 4

Sanctions

Sanctions Act 1977, DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act 9

4.1 The Sanctions Act 1977 (SW) and the regulations derived from it transpose international sanction regimes, especially those of the United Nations and the European Union, into Dutch law. The Regulation on Supervision pursuant to the Sanctions Act 1977 (Regeling Toezicht Sanctiewet 1977) prescribes that an institution must take measures to screen whether relationships of the institution appear on one or more sanction lists (such as EU decisions and/or regulations, decisions by the Dutch Minister of Foreign Affairs based on the Dutch regulation on terrorism sanctions 'Sanctieregeling Terrorisme 2007-II' – also referred to as the 'Dutch List' – or UN Security Council Resolutions). The European Union Regulations describe several financial sanctions:

- An order to freeze funds and assets of designated persons or organisations;
- A ban on making resources available to these persons or organisations directly or indirectly;
- A ban or restrictions on providing financial services.

Finacial institutions may also consider, as part of their risk appetite, to comply with OFAC sanctions, as long as these sanctions are not contradictory with EU and/or Dutch sanctions regulations.

Sanction hits

Sanctions Act 1977

4.2 Banks must take measures to ensure that they can identify relationships that correspond with natural or legal persons and entities as referred to in the sanctions regulations. Banks must subsequently ensure that they do not provide financial resources or services to those relationships and that they are able to freeze their financial assets immediately. It is not permitted to exit an existing client and in case of a freeze other than an exemption is granted from the ministry of Finance. If the bank establishes that a relationship's identity corresponds with that of a natural or legal person or entity as referred to in the sanction's regulations (only genuine hits are reported; 'false positives' are not), the bank must

report this immediately to the competent authorities using the prescribed report form.

4.3 In the event of a sanction's hit, the bank reports the following to the supervisor:

- Identifying information (name, alias, address, place and date of birth);
- The amount and nature of the funds or assets frozen;
- The action taken by the institution;
- The number of the applicable sanction regulation.[38]

4.4 Banks use the report format drawn up by AFM and DNB to report a hit to the relevant competent authority. DNB assesses the reports received from banks. In the event of a genuine hit, DNB will forward the report to the Ministry of Finance. If DNB believes, in assessing the report, that it is not a hit the report will not be forwarded to the Ministry of Finance. In both cases the reporting bank will be advised accordingly.

Exemptions are possible in some cases (this may vary depending on the sanction regulation). The Minister of Finance is authorized to decide on this. A substantiated request for exemption can be sent to the Ministry of Finance).

Meanwhile, it appears only to be expected that where a bank freezes assets on the basis of a match with the 'terrorist lists', it will also look at the owner's transaction history to see whether any transactions have occurred that warrant the conclusion that they may have been made in connection with TF. In case of a suspicion of TF, the bank will report those transactions to the FIU in accordance with the Wwft.

Assets remain frozen until the relevant sanctions regulation is changed and the obligation to freeze the assets is lifted, an exemption is granted or if otherwise notice to the contrary is received from the Ministry of Finance or the supervisory authorities. If the institution does not hear anything, it can assume that the assets are to be considered an actual 'hit' and should remain frozen until further notice.

.....

[38] http://www.toezicht.dnb.nl/en/2/51-221960.jsp

The reported data must be kept for a period of five years after the relevant sanctions regulation has ceased to have effect or has been rendered inoperative.

Sanctions and penalties

4.5 Not reporting an unusual transaction, while the bank is familiar with the unusual nature of the transaction, is an economic offence.

Financial sanctions legislation

4.6 If a bank fails to comply with the obligations to freeze funds, not to make funds, economic resources and, in relation to suspected terrorists, financial services, available to listed persons or entities or to report knowledge or suspicion, it is open to prosecution.

Chapter 5

Staff awareness and training

Wwft 35

5.1 One of the most important controls over the prevention and detection of ML/TF is to have staff who are alert to the risks of ML/TF and well-trained in the identification of unusual activities or transactions which may be suspicious and to adequately execute CDD measures for which they are responsible.

5.2 The effective application of even the best-designed control systems can be quickly compromised, if the relevant staff applying the systems are not adequately trained. The content and effectivenesss of such training will therefore be important to the success of the bank's AML/CTF strategy. The following paragraphs 5.3 to 5.14 are considered to be best practices for setting up and excuting training and awareness activities in line with the requirements of Wwft article 35.

5.3 It is essential that banks implement a clear and well-articluated policy to ensure that relevant employees are aware of their obligations in respect of the prevention of ML/TF and for training them in the identification and reporting of anything that gives grounds for suspicion. This is especially important for staff who directly handle customer transactions or instructions. Temporary and contract staff carrying such functions must also be covered by these training programs.

5.4 It is important that banks inform their employees that they might be held personally liable:

- For the failure to report any knowledge or suspicion of ML/TF in accordance with the Wwft;
- If they deliberately avoid or ignore information that could have led to the discovery of unlawful activity, so-called "willful blindness".

5.5 In determining the nature and extent of AML/CTF training measures, banks may take account of the nature and size of their businesses and the nature and extent of the risks of ML/TF to

which their businesses is subject. Records of training measures taken must be kept.

5.6 Sufficient training will need to be given to all relevant employees to enable them to identify unusual transactions that may involve ML/TF.

5.7 Banks will need to train employees, in particular, on how products and services may be used as a vehicle for ML/TF. Employees must be trained in the bank's procedures for managing this risk.

5.8 Relevant employees will need to be trained in what they need to know in order to carry out their particular role. Staff involved in customer acceptance, risk assessment, customer servicing or settlement functions will need different training, tailored to their particular function. This may involve making them aware of the importance of CDD requirements for ML/TF prevention purposes, and of the respective importance of customer identification and verification procedures, obtaining additional information and monitoring customer activity. The awareness raising and training in this respect will need to cover the verification of the identity of the customer and circumstances when it is necessary to obtain appropriate and additional customer information in the context of the nature of the transaction or the customer relationship concerned.

5.9 Relevant employees also need to be made aware of the particular circumstances of customers who present a higher risk of ML/TF and how best to identify these. Training needs to include how identity should be verified in such cases, what additional steps can be taken, and what (local) check can be made.

5.10 Staff awareness and training programmes also include the nature of terrorism funding and terrorist activity, in order that staff are alert to customer transactions or activities that might be terrorist-related.

5.11 It is important that staff are appropriately made aware of changing behavior and practices amongst money launderers and those financing terrorism. Refer for more information to the different typology reports published by FATF.

5.12 There is no single solution when determining how to deliver training; a mix of training techniques may be appropriate. Online

learning systems can often provide an adequate solution for many employees, but there will be classes of employees for whom such an approach is not suitable. Focused classroom training for higher risk or minority areas can be more effective.

5.13 Ongoing training can best be given at appropriate intervals to all relevant employees. This may take, particularly in larger banks, the form of a rolling programme.

5.14 Whatever the approach to training, it is vital to establish comprehensive records to monitor who has been trained, when they received the training, the nature of the training given and its effectiveness.

Chapter 6

Record Keeping

Relevant law/regulation

- Wwft, Article 1e, 2b, 2f, 10, 33, 34, 34a
- DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act – section 7
- EU Regulation 2015/847 on information accompanying transfers of funds, Art. 16
- Algemene verordening gegevensbescherming / GDPR
- Section 10, Book 2 of the Netherlands Civil Code (Burgerlijk Wetboek / BW), Section 52 of the State Taxes Act (Algemene Wet inzake Rijksbelastingen / AWR)

Core obligations

- Banks must retain:
  - All data and information obtained during the CDD process to satisfy the CDD measures, e.g. copies of, or references to, the evidence they obtained of a customer's identity, for five years after the end of the customer relationship;
  - Details of customer transactions for five years from the date of the transaction;
- Banks must retain:
  - Details of actions taken in respect of internal and external suspicion reports;
  - Details of information considered by the nominated officer in respect of an internal report where no external report is made;
- Banks must delete any personal data relating to CDD and customer transactions, upon expiry of the retention period, unless otherwise prescribed by law.

Actions required, to be kept under regular review

- Banks maintain appropriate systems for retaining records;
- Banks maintain appropriate systems for making records available when required, within the specified timescales.

General legal and regulatory requirements

Wwft 33, 34

6.1 This chapter provides guidance on appropriate record keeping procedures that will meet a bank's obligations in respect of the prevention of ML/TF. There are general obligations for banks to maintain appropriate records and controls more widely in relation to their business; this guidance is not intended to replace or interpret such wider obligations. Therefore, each bank is responsible for developing their own record retention policies and procedures according to the nature of their business.

6.2 Record keeping is an essential component of the audit trail that the Wwft requirements seek to establish in order to assist in any financial investigation and to ensure that criminal funds are kept out of the financial system, or if not, that they may be detected and confiscated by the authorities.

Wwft 1e, 2b, 2f, 10

6.3 Apart from legislation for record keeping in relation to customer identification and transactions with customers, there are obligations for banks to document their risk assessment, and their group-wide policies, controls and procedures. A bank is also required to have written arrangements with any third party on which they rely to apply CDD measures.

6.4 Banks must retain records concerning customer identification and transactions as evidence of the work they have undertaken in complying with their legal and regulatory obligations, as well as for use as evidence in any investigation conducted by law enforcement.

Banks must take reasonable care to make and keep adequate records appropriate to the scale, nature and complexity of their businesses.

General records to be kept by banks

Wwft 33

6.5 The precise nature of the records required is not specified in the legal and regulatory regime. The objective is to ensure that a bank meets its obligations and that, in so far as is practicable, in any subsequent investigation the bank can provide the authorities with its section of the audit trail.

6.6 The bank's records should cover information related to AML/CTF and sanctions obligations in the following areas:

- Customer information;
- Transactions;
- Screening and monitoring records;
- Internal and external reports;
- Nominated officer Compliance monitoring;
- Training and awareness.

Customer information

Wwft 33

6.7 In relation to the evidence of a customer's identity, a bank must keep a copy of any documents, data or information it obtained to satisfy the CDD measures required under the Wwft.

6.8 A bank may often hold additional information with respect to a customer obtained for the purposes of enhanced customer due diligence or ongoing monitoring.

6.9 The customer file should also reveal how the decision-making process surrounding customer acceptance has taken place, e.g. in the case of high-risk customers.

Wwft 33

6.10 Records of identification evidence must be kept for a period of five years after the customer relationship with the customer has ended, i.e. the closing of the account or accounts, or after the occasional transaction was carried out.

Banks must retain these data for at least five years following termination of the customer relationship or following the provision of services.

In the case of a non-recurring transaction, the period of data retention should be at least five years after the transaction was carried out.

Wwft 34a(3)

6.11 Upon the expiry of the five-year period referred to in paragraph 6.10, banks must delete any personal data unless:

- The bank is required to retain records containing personal data by, or under, any enactment, or for the purposes of any court proceedings; or
- The bank has reasonable grounds for believing that records containing the personal data need to be retained for the purpose of legal proceedings; or
- Otherwise prescribed by law.

The Guidelines 'Identification and verification of personal data' of the Dutch Data Protection Agency (College Bescherming persoonsgegevens, CBP) state that a financial institution – as proof of the identification requirement (duty to reproduce) – can document a copy of the verified identity document. Based on the Wwft, Section 33, there is no requirement to document the citizen service number (burgerservicenummer, BSN).

Wwft 34

6.12 A bank that is relied on by another bank for the purposes of CDD must keep the records for five years from the ending of the customer relationship with the customer.

6.13 Where documents verifying the identity of a customer are held in one part of a group, they do not need to be held in duplicate form in another. The records do, however, need to be easily accessible to the supervisory authorities and to all areas that have contact with the customer, and be available upon request, where these areas seek to rely on this evidence, or where they may be called upon by law enforcement to produce them. The various records and files should therefore be easily accessible to the supervisory authorities. It makes no difference whether the data are stored electronically or as a physical document.

6.14 When an introducing branch or subsidiary undertaking ceases to trade or have a customer relationship with a customer, if his relationship with other group members continues, particular care needs to be taken to retain, or hand over, the appropriate customer records. Similar arrangements need to be made if a company holding relevant records ceases to be part of the group. This will also be an issue if the record keeping has been delegated to a third party.

Transactions

EU Regulation 2015/847 on information accompanying transfers of funds, 16

6.15 All transactions carried out on behalf of or with a customer in the course of relevant business must be recorded within the bank's records. Transaction records in support of entries in the accounts, in whatever form they are used, e.g. credit/debit slips, cheques, must be maintained in a form from which a satisfactory audit trail can be compiled where necessary, and which may establish a financial profile of any suspect account or customer.

EU Regulation 2015/847 on information accompanying transfers of funds 16

6.16 Records of all transactions relating to a customer must be retained for a period of five years from:

- Where the records relate to an occasional transaction, the date when the transaction is completed; or
- In other cases, the date the customer relationship ended, i.e. the closing of the account or accounts.

EU Regulation 2015/847 on information accompanying transfers of funds16

6.17 Upon the expiry of the period referred to in paragraph 4.16, banks must delete any personal data unless:

- The bank is required to retain records containing personal data by, or under, any enactment, or for the purposes of any court proceedings; or
- The bank has reasonable grounds for believing that records containing the personal data need to be retained for the purpose of legal proceedings; or
- Otherwise prescribed by law.

Internal and external reports Wwft 34

6.18 A bank must make and retain:

- Records of actions taken under the internal and external reporting requirements; and
- When the nominated officer has considered information or other material concerning possible ML/TF, but has not made a report to the FIU, a record of the other material that was considered.

6.19 In addition, copies of any SARs made to the FIU must be retained, including:

- All information which is required to reconstruct the transaction;
- A copy of the SAR filing itself (note the confidentiality requirement of SARs);
- The notification from the FIU confirming the receipt of the SAR.

6.20 Records of all internal and external reports must be retained for at least five years from the date the report was made, or from the date when the notification from the FIU was received.

Other

6.21 A bank's records may consider:

(a) In relation to training:

- Dates of training;
- The nature of the training, and involved staff;
- The results of the tests undertaken by staff, where appropriate.

(b) In relation to compliance monitoring:

- Reports by the nominated officer to senior management; and
- Compliance monitoring plans

Wwft 33

6.22 A bank must establish and maintain systems that enable it to respond fully and rapidly to enquiries from the FIU and/or the competent authority whether it maintains, or has maintained during the previous five years, a customer relationship with any person and the nature of that relationship.

Form in which records have to be kept

6.23 Most banks have standard procedures that they keep under review and will seek to reduce the volume and density of records that have to be stored, whilst still complying with Wwft requirements. Retention may therefore be:

- By way of original documents;
- By way of photocopies of original documents;
- On microfiche;
- In scanned form;
- In computerized or electronic form.

6.24 The record retention requirements are the same, regardless of the format in which they are kept, or whether the transaction was undertaken by paper or electronic means.

6.25 Banks involved in mergers, take-overs or internal reorganizations need to ensure that records of identity verification and transactions are readily retrievable for the required periods when rationalizing computer systems and physical storage arrangements.

Location

6.26 The Wwft does not state where relevant records should be kept, but the overriding objective is for banks to be able to retrieve relevant information without undue delay.

6.27 Where identification records are held outside the Netherlands, it is the responsibility of the Dutch bank to ensure that the records available do in fact meet Wwft requirements. No secrecy or data protection legislation should restrict access to the records either by the Dutch regulated bank freely upon request, or by Dutch law enforcement agencies under court order or relevant mutual assistance procedures. If it is found that such restrictions exist, copies of the underlying records of identity should, wherever possible, be sought and retained within the Netherlands.

6.28 Banks should take account of the scope of AML/CTF legislation in other countries and should ensure that group records kept in other countries that are needed to comply with Dutch legislation are retained for the required period.

6.29 There can be some tension between the provisions of the Wwft and data protection legislation; the nominated officer has to balance between both sets of obligations.

6.30 When setting document retention policy, banks must weigh the statutory requirements and the needs of the investigating authorities against normal commercial considerations. When original vouchers are used for account entry and are not returned to the customer or his agent, it is helpful to the law enforcement agencies if these original documents are kept for forensic analysis. This can also provide evidence for banks when conducting their own internal investigations. However, this is not a requirement of the AMLCTF legislation, and retaining electronic/digital copies may be a more realistic storage method.

Sanctions and penalties

6.31 Where the record-keeping obligations under the Wwft are not observed, a bank or person is open to prosecution, including imprisonment /or a fine, or regulatory censure. Management and/ or staff of a bank may also be held accountable by their employer for failure to comply with external and or internal record-keeping requirements.

Glossary of terms

Term	Definition
Authorised representatives	Persons who represent the customer towards the bank at customer relationship level concerning dedicated legal responsibilities and who are delegated by the direct appointees to represent the customer, either for the whole relationship or for a specific product or service: these include authorised signatories, proxy holders, holders of a power of attorney, etc.
Bank	A credit institution as defined in Article 4 of the Capital Requirement Regulation. (Regulation (EU) No. 575/2013). Unless determined otherwise the holder of a licence as referred to in Article 3:4 Wft shall be treated in the same way as a bank. *[Article 1.1 Wft]*
Basel Committee	Basel Committee on Banking Supervision.
Commercial real estate	Commercial real estate activities are defined as: • Project development in the commercial real estate sector; • Financing and co-financing of investment assets, investment objects, development products or project development related to the commercial real estate sector; • Investments in the commercial real estate sector. *[Art. 1 DNB Beleidsregel Integriteitbeleid ten aanzien van zakelijke vastgoedactiviteiten]*
Complex entity	A legal entity or arrangement that is less transparent and where ownership, control and profit interests are spread over different roles, e.g. trusts, limited partnerships (e.g. CV), foundations, anstalt, LLCs, funds, cooperatives, etc.
Criminal property	Property which constitutes a person's benefit from criminal conduct or which represents such a benefit (in whole or part and whether directly or indirectly), and the alleged offender knows or suspects that the property constitutes or represents such a benefit. *[Wetboek van strafrecht]* *[Money Laundering: Article 420 bis Wetboek van Strafrecht]*
Criminal conduct	Conduct that constitutes an offence in any part of the Netherlands, or would constitute an offence in any part of the Netherlands if it occurred there. *[Wetboek van Strafrecht]*

Customer	A natural person or legal entity with whom a customer relationship is established, or on whose behalf a transaction is executed. *[Article 1.1 Wwft]*
Customer Relationship	Business, professional or commercial relationship, which is connected with the professional activities (meaning a banking activity in the context of the Wwft) of an obliged entity and which is expected, at the time when the contact is established, to have an element of duration, for which the Wwft is applicable. *[Article 1.1 Wwft]*
DNB Guidance AML/CTF and sanctions	DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act Preventing the misuse of the financial system for ML/TF purposes and controlling integrity risks
DNB Guidance PTM	DNB Guidance on Post-event transaction monitoring process for banks
EU Sanctions Regulation	Regulation 2580/2001, on specific restrictive measures directed against certain persons and entities with a view to combating terrorism.
Equivalent or low risk jurisdictions;	Third countries with effective AML/CTF regimes *[Annex II Directive (EU) 2015/849]*
European Economic Area (EEA)	Member States of the European Union, plus Iceland, Liechtenstein and Norway.
Equivalent country	Refers to a country that has an equivalent AML/CTF system to the EU. For practical purposes this means any country that has one or more regulators on the Recognised Regulators List.
Express trust	A trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts that come into being through the operation of the law and that do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g. constructive trust).
FATF Recommendations	The FATF Recommendations set out a comprehensive and consistent framework of measures that countries should implement in order to combat ML/TF, as well as the financing of proliferation of weapons of mass destruction. Countries have diverse legal, administrative and operational frameworks and different financial

	systems, and so cannot all take identical measures to counter these threats. The FATF Recommendations, therefore, set an international standard, which countries should implement through measures adapted to their particular circumstances. The FATF Standards comprise the Recommendations themselves and their Interpretive Notes, together with the applicable definitions in the Glossary.
Financial Institution	An undertaking (other than a bank) that carries out one or more of the operations (other than trading on their own account where the undertaking's only customers are group companies) listed in 2 - 12 and 15 of Annex I of the Capital Requirements Directives (Directive 2013/36/EU) *[Article 1.1 Wft]*
Firm	1. a firm mentioned in article 1a (4)(a), (b), (c), (d), (e) Wwft established in the NL or in another member state; 2. a firm mentioned in article 1a (4)(f) Wwft who has a license as referred to in article 2 (1) or (2) "Wet toezicht trustkantoren (wtt)"; 3. a firm as referred to in article 1a (2) and (3) Wwft or a branch of that firm established in the NL or in another member state; 4. a firm mentioned under (1) and (3) above who carries on business in a third country as designated by the Dutch Minister of Finance not being a member state and who is subject to, and supervised for compliance with, CDD and record keeping requirements equivalent to those laid down in Wwft. (Currently there are no countries designated by the minister).
Government-issued	Issued by a central government department or by a local government authority or body.
Identification	Ascertaining the name of, and other relevant information about, a customer or beneficial owner.
Legal representatives	Those individuals who, individually or collectively, exercise practical control over a non-personal entity.
Money laundering	Criminal Conduct which covers at least the following: a) The conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;

	b) The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity; c) The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity; d) Participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to above; e) Any of the actions referred to above, where a person does not know but should reasonably have suspected that the property is derived from criminal activity. *[Article 420bis, 420bis.1, 420ter, 420quater, 420quater.1 Wetboek van Strafrecht* *Article 1.1 Wwft]*
Money service business	Any person or entity doing business, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities: • Currency dealer or exchanger, e.g. bureaux de change • Check casher • Issuer of traveller's checks, money orders or stored value • Seller or redeemer of traveller's checks, money orders or stored value • Money transmitter, including payment service providers and administrators and exchangers of virtual currencies, e.g. Bitcoins. *[Article 1.1 Wft]*
Nominated officer	A person in a bank or organisation nominated by the bank or organisation to receive disclosures under Regulation 21(5) and s 330 of POCA from others within the bank or organisation who know or suspect that a person is engaged in ML . Similar provisions apply under the Terrorism Act.
Nominee director	Refers to a Trust Company Service Provider (TCSP) , a representative of a TCSP or other professional intermediary acting as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons.
Nominee shareholder	A nominee shareholder refers to a company member holding the shares on behalf of the actual owner or beneficial owner. S/he is the registered owner of the share. Formal nominee shareholder: Stock (shares) purchased through or placed with a nominee (attorney, bank, broker, etc.) whose name appears as the registered owner of the shares (instead of the name of their actual or beneficial owner). A formal nominee shareholder holds the share under a custodial agreement.

	Informal nominee shareholder (“front men”): Close associates and family members that are the registered owners on behalf of the actual beneficial owner, who in this way tries to shield his identity from the authorities.
Non-transparant jurisdiction	Non-transparent jurisdictions countries and territories that have high levels of secrecy and that claim little or no tax from certain entity types (e.g. exempt companies or IBCs). In particular the use of jurisdictions that are deemed not compliant by the OECD and the EU with international tax transparency and information sharing standards should be treated as a serious red flag.
Occasional transaction	Any transaction that is not carried out as part of a customer relationship. *[Article 3 lid 5 sub b and g Wwft]*
Ownership interest	Any transaction that is not carried out as part of a customer relationship. *[Article 3 lid 5 sub b and g Wwft]*
Politically exposed person	PEPs, also referred to in certain jurisdictions as Senior Foreign Political Figures, are individuals holding or having held positions of public trust, as well as close family members and close associates of such individuals. They may appear as a customer, ultimate beneficial owner of a customer, principal or person authorised to act on behalf of the customer. PEPs includes the following positions: a) Heads of State, heads of government, ministers and deputy or assistant ministers; b) Members of parliaments or of similar legislative bodies; c) Members of the governing bodies of political parties; d) Members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances; e) Members of courts of auditors or of the boards of central banks; f) Ambassadors, chargés d'affaires, and high-ranking officers in the armed forces; g) Members of the administrative, management or supervisory bodies of State owned enterprises; h) Directors, deputy directors and members of the board or equivalent function of an international organisation. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories. Family members include the PEP’s direct family members including spouses or partners, children and their spouses or partners, and parents of the PEP. Close associates include (i) any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements; (ii) any natural person who has sole beneficial

	ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of a PEP. Although some countries restrict their definition of a PEP to foreign political figures, the inherent risks associated with PEPs are present regardless of whether the PEP is a domestic national official or a foreign official. Accordingly, the status of the individual being domestic or foreign is irrelevant in deciding whether someone is a PEP, but this can weigh in the measures that need to be applied to the PEP. It is irrelevant whether the role is one to which the individual has been elected, appointed or which is the result of heritage. A PEP will be considered a PEP for as long as that person continues to pose the risk specific to PEPs and at least for a period of one year after the public function ceases. *[Article 1.1 Wwft]* *[Article 2 Uitvoeringsbesluit Wwft 2018]*
Private Banking	Wealth management is the provision of banking and other financial services to high-net- worth individuals and their families or businesses. It is also known as private banking. Clients of wealth management firms can expect dedicated relationship management staff to provide tailored services covering, for example, banking (e.g. current accounts, mortgages and foreign exchange), investment management and advice, fiduciary services, safe custody, insurance, family office services, tax and estate planning and associated facilities, including legal support. The risk is primarily related to (international) private banking services where there is close contact with the customer and intensive advising by the bank.
Privately-Held Multinational	A privately-held commercial entity belonging to a group that: 1. Has a customer based in an EEA or OECD country; and 2. Is active in at least three countries; and 3. Has an annual turnover of USD 1b or more; and 4. Is audited by a reputable international accountancy firm.
Recognised Exchanges List	A financial institution's approved list of stock exchanges that are subject to disclosure requirements consistent with EU law or that it considers to be subject to equivalent international standards which ensure adequate transparency of ownership information.
Recognised Exchange Listed Entity	An entity whose shares are listed on a regulated market that is subject to disclosure requirements consistent with EU law or subject to equivalent international standards that ensure adequate transparency of ownership information (see also the Recognised Exchanges List). This includes also the wholly100% -owned and controlled subsidiaries of such entities.

Recognised Regulators List	A financial institution's approved list of regulators from the EEA and from countries that it considers having an equivalent AML/CTF system to the EU.
Recognised Regulated Entity	A financial institution that is regulated by a regulator from the EEA or a country with an equivalent AML/CTF system (the Recognised Regulators List).
Regulated market	A multilateral system operated and/or managed by a market operator, which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments - in the system and in accordance with its non-discretionary rules - in a way that results in a contract, in respect of the financial instruments admitted to trading under its rules and/or systems, and which is regulated and functions regularly [and in accordance with the provisions of Articles 36-47 of MiFID]. *[MiFID Article 4(14)]*
Senior management	In the sense of approval for certain types of customer relationship, an officer or employee of a bank in the regulated sector with sufficient knowledge of the bank ML/TF risk exposure, and of sufficient authority, to take decisions affecting its risk exposure.
Senior managing official (*hoger leidinggevend personeel*)	In the context of pseudo-UBOs, Senior managing officials are defined as: a. persons who determine the day-to-day policy of an institution; or b. persons working under the responsibility of an institution, who fulfil a management function directly under the echelon of the day-to-day policymakers and who are responsible for natural persons whose activities influence the exposure of an institution to the risks of ML/TF. *[Article 1.1 Wwft]*
Shell company	A company that is incorporated that have no significant operations or related assets, often set up in offshore jurisdictions.
Source of funds	The source of funds refers to the activity that generates the funds for a particular customer relationship or occasional transaction.
Source of wealth	The source of wealth relates to the activities that have generated the total net worth of a natural person i.e. those activities that have generated a person's net assets and property.
State-owned entities	Entities that are created to undertake commercial activities on behalf of a government and are majority-owned or controlled by a government.

Transaction	An act or a combination of acts performed by or on behalf of a customer of which the institution has taken note in the provision of its services to that customer. *[Article 1.1 Wwft]*
Terrorist financing	Criminal conduct that covers at least the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any terrorist offences. *[Article 421 of Wetboek van Strafrecht* *Article 1.1 Wwft]*
Terrorist property	• Money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation); or • Proceeds of the commission of acts of terrorism; or • Proceeds of acts carried out for the purposes of terrorism "Proceeds of an act" includes a reference to any property that wholly or partly, and directly or indirectly, represents the proceeds of the act (including payments or other rewards in connection with its commission). "Resources" includes any money or other property which is applied or made available, or is to be applied or made available, for use by the organisation. *[Article 421 Wetboek van Strafrecht]*
Tipping off	A tipping-off offence is committed, if a person knows or suspects that a disclosure falling under Article 15 Wwft and Annex Indicators Uitvoeringsbesluit Wwft 2018 has been made, and he makes a disclosure which is likely to prejudice any investigation which may be conducted following the disclosure under Article 16 Wwft. *[Article 22 Wwft]*
Transaction	Is an act or a combination of acts performed by or on behalf of a customer of which the institution has taken note in the provision of its services to that customer.
Transfer of funds	Any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same, including: (a) a credit transfer as defined in point (1) of Article 2 of Regulation (EU) No 260/2012;

	(b) a direct debit as defined in point (2) of Article 2 of Regulation (EU) No 260/2012; (c) a money remittance as defined in point (13) of Article 4 of Directive 2007/64/EC, whether national or cross-border; (d) a transfer carried out using a payment card, an electronic money instrument, or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics.
Trust Company Service Providers (TCSP)	Entities (e.g. Dutch Trustkantoren) that, among others, carry out the following activities: • acting as a formation agent of legal persons; • acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; • providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; • acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement; • acting as (or arranging for another person to act as) a nominee shareholder for another person.
Ultimate Beneficial owner(s)	Any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted. *[Article 1.1 Wwft]* *[Article 3 Uitvoeringsbesluit Wwft 2018]*
Ultimate parent	Ultimate (Legal) Parent: The top entity in an ownership structure that directly or indirectly owns more than 50% of the shares of the customer. Ultimate Controlling Parent: The top entity in an ownership structure that directly or indirectly controls more than 50% of the voting rights in the customer.
Wwft regulated sector	Persons and banks that are subject to the Wwft.

Abbreviation

AFM	Autoriteit Financiële Markten
AML	Anti-money laundering
CTF	Combating terrorist financing
DNB	De Nederlandsche Bank
ESAs	The European Supervisory Authorities – The European Banking Authority, the European Securities Markets Authority and the European Insurance and Occupational Pensions Authority, working together
FATF	Financial Action Task Force, an intergovernmental body whose purpose is to develop and promote broad AML/CTF standards, both at national and international levels
FIU	Financial Intelligence Unit
MiFID	The Marketing in Financial Instruments Directive
ML	Money Laundering
NVB	Nederlandse Vereniging van Banken
SAR	Suspicious (and Unusual) activity report . Depending on the local context, an unusual transaction report may also be reffered to as SAR/STR/CTR.
SIRA	Systematic Integrity Risk Analysis
TF	Terrorist Financing
UAVG	Uitvoeringswet Algemene verordening gegevensbescherming
Wft	Wet op het financieel toezicht
Wwft	Wet ter voorkoming van witwassen en financieren van terrorisme
SW	Sanctiewet 1977

Annex I - List of Recognised Exchanges

Methodology

The following methodology has been and will be applied for the selection of countries with an adequate transparency regime for the purpose of the List of Recognised Exchanges.

EU/EEA member states

According to the Implementing Decree Wwft 3(1a) there is no obligation to identify UBOs of companies (including (in)direct 100% subsidiaries) listed on a regulated market that is subject to disclosure requirements consistent with Union law or subject to equivalent international standards, which ensure adequate transparency of ownership information. As all EU/EEA members are obliged to implement Directive 2004/109/EC on the harmonisation of transparency requirement in relation to information about issuers whose securities are admitted to trading on a regulated market we consider the regulated markets of the EU/EEA members states to have appropriate standards in place to ensure adequate transparency of ownership information.

OECD Corporate Governance Factbook

The OECD Corporate Governance Factbook was published for the first time in 2014 and is updated regularly. Based on the information in the OECD Factbook the following countries are considered to have equivalent international standards which ensure adequate transparency of ownership information in place: Argentina, Australia, Brazil, Canada, Chile, China, Columbia, India, Indonesia, Israel, Japan, Korea (South), Mexico, New Zealand, Singapore, South Africa, Switzerland, Turkey and United States.

Corporate-Governance-Factbook.pdf

Additional countries

Additional countries can be added to the list after it has been determined that the concerned country meets the criteria as listed below. These requirements are derived from Directive 2004/109/EC. The assessment must be performed based on relevant and current data and information. The assessment must be documented and send to the NVB together with a request to add the country to the list of countries with an adequate transparency regime for the purpose of the List of Recognised Exchanges.

1. Periodic information (refer to article 4 to 6 of Directive 2004/109/EC)

Listed companies on a regulated market are obliged to inform the public on a regular basis. This concerns information related to the financial situation and forecasts of the issuer and the enterprises it controls.

2. Publication of major shareholdings (refer to articles 14, 16 to 18 of Directive 2004/109/EC)
   Listed companies on a regulated market (issuer) must be subject to the obligation to make major shareholdings public. The regulated market imposes an ongoing information requirement whenever events change the breakdown of major holdings that affect the allocation of voting rights. The procedure for notifying and making public major shareholdings involves the new allocation of voting rights, the indentification of the shareholder, the dates of the change and the voting treshold achieved. The information should be made public without delay by the issuer or the competent authority. In addition, the public issuer must make public without delay any change in the rights attaching to the various classes of shares and new loan issues, and in particular any related guarantee or security. Where shares are not admitted to trading on a regulated market, the issuer must make public without delay any changes in the rights of holders of securities other than shares. In all cases, the issuer of securities must ensure equal treatment for all holders of shares who are in the same position.

3. Competent authority (refer to art. 19 of Directive 2004/109/EC)
   There is a competent authority that supervises the compliance with the disclosure requirements. This authority must have all the powers necessary for the performance of its functions, namely:
   - Monitoring of timely disclosure of information by the issuer and publication on its own initiative of information not disclosed within the time limits sets;
   - Request for further information and documents;
   - Verification of compliance with the disclosure requirements, by way of on-site inspections;
   - Suspension for a maximum of ten days of trading in securities or prohibition of trading on a regulated market, if it finds that the disclosure requirements have not been met or if it has reasonable grounds for suspecting that requirements have been infringed.

Country	Exchange	Web address
Argentina	Mercado de Valores de Buenos Aires	www.merval.sba.com.ar
Australia	Australian Stock Exchange	www.asx.com.au
Austria	Wiener Börse	www.wienerborse.at
Belgium	Euronext Brussels	www.euronext.com
Brazil	BM&F Bovespa	www.bmfbovespa.com
Bulgaria	Bulgarian Stock Exchange	www.bse-sofia.bg
Canada	Toronto Stock Exchange	www.tsx.com
Chile	Bolsa Comercio de Santiago	www.bolsadesantiago.com
China	Shanghai Stock Exchange	www.sse.com.cn
	Shenzhen Stock Exchange	www.szse.cn
Colombia	Bolsa de Valores de Colombia	www.bvc.com.co
Croatia	Zagreb Stock Exchange	http://zse.hr/default.aspx?id=64274
Cyprus (Republic of)	Cyprus Stock Exchange	www.cse.com.cy
Czech Republic	Prague Stock Exchange	www.pse.cz
Denmark	Nasdaq OMX Copenhagen	www.nasdaqomxnordic.com
Estonia	Nasdaq OMX Tallinn	www.nasdaqomxbaltic.com
Finland	Nasdaq OMX Helsinki	www.nasdaqomxnordic.com
France	Euronext Paris	www.euronext.com
Germany	Deutsche Börse	www.deutsche-boerse.com
Greece	Athens Exchange	www.helex.gr
Hungary	Budapest Stock Exchange	www.bse.hu
Iceland	Nasdaq OMX Iceland (ICEX)	www.nasdaqomxnordic.com
India	National Stock Exchange JSC	www.nseindia.com
	Bombay Stock Exchange	www.bseindia.com
Indonesia	Indonesia Stock Exchange	www.idx.co.id/en-us/
Ireland	Irish Stock Exchange	www.ise.ie
Israel	Tel Aviv Stock Exchange	www.tase.co.il
Italy	Borsa Italiana	www.borsaitaliana.it
Japan	Tokyo Stock Exchange	www.jpx.co.jp
Korea South	Korea Exchange (KOSPI)	www.krx.co.kr.
Latvia	Nasdaq OMX Riga	www.nasdaqomxbaltic.com
Lithuania	Nasdaq OMX Vilnius	www.nasdaqomxbaltic.com
Luxembourgh	Bourse de Luxembourg	www.bourse.lu
Malta	Malta Stock Exchange	www.borzamalta.com.mt
Mexico	Bolsa Mexicana de Valores	www.bmv.com.mx/en
Netherlands	Euronext Amsterdam	www.euronext.com
New Zealand	New Zealand Exchange	www.nzx.com
Norway	Oslo Bors	www.oslobors.no
Poland	Warsaw Stock Exchange	www.gpw.pl

Country	Exchange	Web address
Portugal	Euronext Lisbon	www.euronext.com
Romania	Bucharest Stock Exchange	www.bvb.ro
Singapore	Stock Exchange of Singapore	www.sgx.com
Slovakia	Bratislava Stock Exchange	www.bsse.sk
Slovenia	Ljubljana Stock Exchange	www.ljse.si
South Africa	Johannesburg Stock Exchange	www.jse.co.za/
Spain	Bolsas y Mercados Españoles	www.bolsasymercados.es
Sweden	Nasdaq OMX Stockholm	www.nasdaqomxnordic.com
Switzerland	SIX Swiss Stock Exchange	www.six-swiss-exchange.com
Turkey	Borsa Istanbul	www.borsaistanbul.com/en/home-page
United Kingdom	London Stock Exchange	www.londonstockexchange.com
United States	New York Stock Exchange	www.nyse.com
	NASDAQ Stock Market	www.nasdaqomx.com

Annex II - List of Recognised Regulators

Methodology

The following methodology has been and will be applied for the selection of countries with an adequate transparency regime for the purpose of the List of Recognised Exchanges.

EU/EEA member states

Banks may, according to article 5 sub 1a 4 Wwft, rely on financial institutions registered in EU/EEA member states.

Equivalent countries

Next to EU/EEA member states reliance may be placed on countries that apply CDD requirements and record-keeping requirements consistent with those laid down in EU Directive 2015/849. Countries that are members of the OECD and/or FATF are considered to have an AML/CTF regime equivalent to that of the EU/EEA members states. Russia is excluded from this list due to the Ukraine-related sanctions imposed on the country by the EU.

Country	Regulator	Web address
Argentina	Central Bank of Argentina	www.bcra.gob.ar
Australia	Australian Prudential Regulation Authority	www.apra.gov.au
	Reserve Bank of Australia	www.rba.gov.au
	Australian Securities and Investments Commission	http://www.asic.gov.au
Austria	Austrian Financial Market Authority	www.fma.gv.at
	Österreichische Nationalbank (OENB)	www.oenb.at
Belgium	Autoriteit voor Financiële Diensten en Markten (FSMA)	www.fma.gv.at
	National Bank of Belgium	www.oenb.at
Brazil	Commissao do Valores Mobiliarios – Securities and Exchange Commission of Brazil (CVM)	www.cvm.gov.br
	Banco Central do Brasil	www.bcb.gov.br
	Superintendence of Private Insurance	http://www.susep.gov.br

Country	Regulator	Web address
Bulgaria	Financial Supervision Commission	www.osc.gov.on.ca
	Bulgarian National Bank	www.fsco.gov.on.ca
Canada	Office of the Superintendent of Financial Institutions	www.osfi-bsif.gc.ca
	Canadian Securities Administrators: • Alberta Securities Commission • Autorite des Marches Financiers (Quebec) • British Columbia Securities Commission • Ontario Securities Commission	www.securities-administrators.ca www.albertasecurities.com https://lautorite.qc.ca https://www.bcsc.bc.ca https://www.osc.gov.on.ca
	Financial Services Commission of Ontario	http://www.fsco.gov.on.ca
	Investment Industry Regulatory Organization of Canada	http://www.iiroc.ca
	Mutual Fund Dealers Association of Canada	http://mfda.ca/
Chile	Superintendencia de Bancos e Instituciones Financieras Chile	https://www.sbif.cl
	Superintendencia de Pensiones	http://www.safp.cl
	Unidad de Análisis Financiero	http://www.uaf.cl
China	The People's Bank of China	http://www.pbc.gov.cn
	China Banking Regulatory Commission	http://www.cbrc.gov.cn
Croatia	Croatian Financial Services Supervisory Agency (HANFA)	https://www.hanfa.hr
	Croatian National Bank	http://www.hnb.hr
Cyprus (Republic of)	Central Bank of Cyprus	https://www.centralbank.cy
	Cyprus Securities and Exchange Commission	https://www.cysec.gov.cy
Czech Republic	Czech National Bank	www.cnb.cz
Denmark	Finanstilsynet (Danish Financial Supervisory Authority)	www.ftnet.dk
	National Bank of Denmark	www.nationalbanken.dk
Estonia	Bank of Estonia	https://www.eestipank.ee
	Finantsinspektsioon (Estonian Financial Supervision Authority)	www.fi.ee
Finland	Financial Supervision Authority (FIN-FSA)	https://www.finanssivalvonta.fi

Country	Regulator	Web address
France	Banque de France	https://acpr.banque-france.fr
	Autorité des Marchés Financiers	www.amf-france.org
Germany	BaFin – Bundesanstalt für Finanzdienstleistungsaufsicht	www.bafin.de
	Deutsche Bundesbank	www.bundesbank.de
Greece	Hellenic Republic Capital Market Commission	http://www.hcmc.gr
	Bank of Greece	https://www.bankofgreece.gr
Hong Kong	Hong Kong Monetary Authority	https://www.hkma.gov.hk
	Securities and Futures Commission	https://www.sfc.hk/web/EN/index.html
	Office of the Commissioner of Insurance	http://www.oci.gov.hk
Hungary	National Bank of Hungary	https://www.mnb.hu
Iceland	FME (The Financial Supervisory Authority)	www.fme.is
India	Reserve Bank of India	http://www.rbi.org.in
	Securities and Exchange Board of India	https://www.sebi.gov.in
	Insurance Regulatory and Development Authority of India	http://www.irdai.gov.in
Ireland	Central Bank of Ireland (includes Irish FSRA)	https://www.centralbank.ie
Israel	Israel Securities Authority	https://www.gov.il
	Bank of Israel	https://www.boi.org.il
Italy	Banca d'Ítalia	http://www.bancaditalia.it/
	Commissione Nazionale per le Società e la Borsa (Consob)	http://www.consob.it/
	Supervision of Insurance	http://www.ivass.it
Japan	Financial Services Agency	https://www.fsa.go.jp/
	Securities and Exchange Surveillance Commission (SESC)	https://www.fsa.go.jp
	Bank of Japan	http://www.boj.or.jp/en
Korea, South	Bank of Korea	https://www.bok.or.kr/eng
	Financial Supervisory Service	http://english.fss.or.kr
Latvia	Financial and Capital Market Commission	http://www.fktk.lv/lv/
	The Bank of Latvia	http://www.bank.lv

Country	Regulator	Web address
Lithuania	Bank of Lithuania	https://www.lb.lt
Luxembourgh	Central Bank of Luxembourg	http://www.bcl.lu/fr/index.html
	Commission de Surveillance du Secteur Financier (CSSF)	http://www.cssf.lu/
	Insurance Commission	http://www.commassu.lu/
Malaysia	Central bank of Malaysia	http://www.bnm.gov.my/
	Labuan Financial	https://www.labuanibfc.com
Malta	Central Bank of Malta	https://www.centralbankmalta.org/
	Malta Financial Services Authority	https://www.mfsa.com.mt
Mexico	Comisión Nacional Bancaria y de Valores (CNBV)	https://www.gob.mx/cnbv
	Banco de México	http://www.banxico.org.mx/
	Comisión Nacional de Seguros y Fianzas	https://www.gob.mx/cnsf
Netherlands	De Nederlandsche Bank	www.dnb.nl
	The Netherlands Authority for the Financial Markets	www.afm.nl
New Zealand	Reserve Bank of new Zealand	https://www.rbnz.govt.nz/
	Financial Markets Authority	https://www.fma.govt.nz/
Norway	Finanstilsynet (Financial Supervisory Authority of Norway)	https://www.finanstilsynet.no/
	Central Bank of Norway (Norges Bank)	https://www.norges-bank.no/
Poland	Polish Financial Supervision Authority (KNF)	https://www.knf.gov.pl/
	National Bank of Poland	http://www.nbp.pl/
Portugal	Portugese Securities Markets Commission (CMVM)	https://www.cmvm.pt/pt/Pages/home.aspx
	Bank de Portugal	https://www.bportugal.pt/en
Romania	Romanian Financial Supervisory Authority	https://asfromania.ro/en/
	National Bank of Romania	https://www.bnro.ro/Home.aspx
Singapore	Monetary Authority of Singapore	www.mas.gov.sg
Slovakia	National Bank of Slovakia	https://www.nbs.sk/en/home
Slovenia	Bank of Slovenia	https://www.bsi.si/en/
	Securities Market Agency	www.a-tvp.si
South Africa	South African Reserve Bank	www.reservebank.co.za
	Financial Services Board	http://www.fsb.co.za/

Country	Regulator	Web address
Spain	Banco de España	https://www.bde.es/bde/es/
	Dirección General de Seguros y Fondos de Pensiones	http://www.dgsfp.mineco.es/
	Comisión National del Mervaco de Valores (CNMV)	www.cnmv.es
Sweden	Finansinspektionen (Financial Supervisory Authority)	https://www.fi.se/
	Sveriges Riskbank	https://www.riksbank.se/en-gb/
Switzerland	Swiss National Bank	https://www.snb.ch/en/
	Swiss Financial Maket Supervisory Authority (FINMA)	https://www.finma.ch/
	All self-regulatory organisations mentioned on the FINMA website	https://www.finma.ch/en/finma-public/authorised-institutions-individuals-and-products/
Turkey	Central Bank of the Republic of Turkey	http://www.tcmb.gov.tr/
	Banking Regulation and Supervision Agency	http://www.bddk.org.tr/
United Kingdom	Bank of England	https://www.bankofengland.co.uk/
	The Financial Conduct Authority	https://www.fca.org.uk/
United States (In addition each state has its own regulators)	Board of Governors of the Federal Reserve System	https://www.federalreserve.gov/
	Federal Deposit Insurance Corporation	http://www.fdic.gov/
	National Credit Union Administration	http://www.ncua.gov
	National Futures Association	http://www.nfa.futures.org
	U.S. Commodity Futures Trading Commission	http://www.cftc.gov
	Office of the Comptroller of the Currency	https://www.occ.treas.gov/
	Security & Exchange Commission	https://www.sec.gov/
	Financial Crimes Enforcement Network	https://www.fincen.gov/
	Financial Industry Regulatory Authority	http://www.finra.org/
	New York State Department of Financial Services	https://www.dfs.ny.gov/