AML, CTF & Sanctions Guidance

Published by the NVB

19 April 2021

Nederlandse Vereniging van Banken

Content

Preface

This Guidance has been developed by the Dutch Banking 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 sanctions risk associated with a customer relationship or with an occasional transaction. This Guidance also provides an outline of how banks can adjust their customer due diligence ("CDD") measures in a way that is commensurate to the ML/ TF and/ or sanctions risk they have identified. This Guidance also addresses customer tax integrity ("CTI") risks and provides an outline of how banks can adjust their CDD measures in a way commensurate to this risk. The factors and measures described in this Guidance 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.

Regulatory framework

This Guidance is primarily based on Dutch legislation. Banks in the Netherlands have had a long-standing obligation to have effective procedures in place to detect and prevent ML/ TF (and sanctions and CTI) violations. These procedures fall primarily within the scope of the following pieces of legislation and guidances:

- Money Laundering and Terrorist Financing (Prevention) Act, 15 October 2020[1] ;
- Sanctions Act 1977, 21 May 2020[2];
- Financial Supervision Act, 15 October 2020[3];
- Trust Offices Supervision Act 2018, 21 May 2020[4]**;**
- (Dutch) Economic Offences Act, 15 October 2020[5];
- Decree on Prudential Rules for Financial Undertakings;[6]
- Implementation Regulation Wwft;
- Implementation Decree Wwft 2018;
- DNB Guideline on Anti-Money Laundering and Counter Anti-Terrorism Financing Act and Sanctions Act, December 2020[7];
- DNB Guidance Post-event transaction monitoring process for banks, 30 August 2017;
- DNB Good practices Customer tax integrity risk management, 28 August 2019;
- General guidelines Anti-Money Laundering and Counter-Terrorist Financing (Prevention) Act published by Ministry of Finance, 21 July 2020;
- AFM Guidance on on Anti-Money Laundering and Counter Terrorism Financing (Prevention) Act and Sanctions Act, 19 October 2020.

.....

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

[2] Sanctiewet 1977 (hereinafter SW). Dutch sanctions guidelines are based on the Sanctions Act of 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 (hereinafter Wft).

[4] Wet toezicht trustkantoren (hereinafter Wtt).

[5] Wet op de Economische Delicten (hereinafter WED).

[6] Besluit prudentiële regels Wft

[7] DNB Guideline version December 2019 and the main (substantive) changes thereto as included in the DNB Guideline version december 2020.

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

- Directive (EU) 2015/ 849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amended by Directive (EU) 2018/ 843 (hereafter referred to as the EU AML/ CTF Directive);
- Wire Transfer Regulation on information accompanying transfers of funds (Regulation (EU) 2015/ 847);
- European Supervisory Authority (hereinafter ESA) Joint Guidelines under Articles 17 and 18(4) of EU AML/ CTF Directive (JC 2017 37);[8]
- ESA Joint Guidelines under Article 25 of Wire Transfer Regulation;
- ESA Opinion on the use of innovative solutions by credit and financial insitutions when complying with their CDD obligations;
- European Union (hereinafter EU) Sanctions Regulations;
- Financial Action Task Force (hereinafter FATF) 40 Recommendations;
- United Nations (hereinafter UN) Security Council Resolutions;
- The Office of Foreign Assets Control (hereinafter OFAC);
- Basel Committee and its Core Principles;
- UK Joint Money Laundering Steering Group (hereinafter JMLSG) and its recommendations.

Please note that Dutch banks are obliged to apply the legal provisions for the prevention of ML/ TF violations in their branches and majority-owned subsidiaries that are located outside the EU/ EEA, insofar as the law of the country[9] concerned does not stand in the way of this. Should the law of the country concerned prevent the application of the statutory regulations, banks must notify the Dutch Central Bank (De Nederlandse Bank, hereinafter DNB) and take measures to effectively manage the ML/ TF risks. International banks with a registered office in the Netherlands must define the Group policy and procedures for compliance with the Dutch AML/ CTF Act that apply to the entire Group. These banks must also ensure that the Group policy and procedures are enforced effectively.

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 sanctions requirements and systems across the banking sector;
- Provide a common interpretation of the requirements of the relevant law and regulations, and of how they may be implemented in practice;
- Indicate good industry practices 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 that they are used in connection with ML, TF and sanctions risks.

.....

[8] ESA (2017) Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions, available at bit.ly/3aBs3l3.

[9] In this Guidance “country” also refers to “jurisdiction".

Scope of this Guidance

This Guidance sets out what may be expected in relation to the prevention of ML, TF and sanctions violations. Banks are nevertheless, ultimately responsible as to how they apply the requirements of the Dutch AML/ CTF regime and the sanctions requirements to the particular circumstances of the bank, and to their 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 constitutes 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.

This Guidance relates solely to how banks are expected to fulfil their obligations under the AML/ CTF, sanctions law and regulations. The Guidance covers the prevention of ML/ TF and sanctions violations. ML/ TF risks are closely related to the risks of other financial crimes, such as fraud, tax evasion and other predicate offences underlying ML and TF.[10] Predicate offences are not specifically dealt with in this Guidance. This Guidance does, however, apply to dealing with any proceeds of crime that arise from these activities. In 2019 the DNB published a set of Good Practices on Customer tax integrity (CTI) risk management, recognizing the link between ML and tax evasion, and the potential hamful effects of tax avoidance on a bank's reputation as well as on the confidence in the Dutch financial sector. CTI is addressed in a separate chapter in this Guidance. In this Guidance reference is generally made to ML/ TF, understanding that this also covers sanctions and CTI (unless explicitly excluded).

Finally, specific requirements in relation to systems and tooling for customer filtering, transaction filtering and transaction monitoring (e.g. settings, scenarios) fall outside the scope of this Guidance.

How should this Guidance be used?

It is not the intention that banks apply this Guidance without careful consideraiton, or as a checklist of steps to take. Instead, 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 manage risks 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 this Guidance, the term "must" is used, to clearly indicate that these provisions are mandatory. Alternatively, the term "should" is used to indicate ways in which the statutory and regulatory requirements may be satisfied, while allowing for

.....

[10] More guidance on the meaning of "predicate offences" is offered in the Interpretive note to recommendation 3 of the FATF relating to the money laundering offence (available at bit.ly/3mt0IFV) , as well as in the EU 2018/1673 of 23 October 2018 on combating money laundering by criminal law.

alternative means of meeting the requirements. The terms ”must” and “should” in this Guidance should therefore be construed accordingly.

The content of this Guidance

This Guidance is 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 sanctions and CTI) risk associated with individual customer relationships or with occasional transactions.

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

The NVB keeps this Guidance (Part I and Part II) under review and updates it as appropriate. This Guidance is maintained by a working group reporting to the Expert Pool on Statutory Requirements Relating to Financial and Economic Crime[11] of the NVB. The NVB will confer on any changes made to the substance of this Guidance.

.....

[11] Expertpool Wet en Regelgeving Criminaliteit (hereinafter EPWRC).

Chapter 1

Risk-based approach

1.1 Introduction and legal obligations

General

1.1.1 There are a number of discrete steps to be taken when assessing the most cost effective and proportionate way to manage and mitigate the money laundering, terrorist financing, sanctions risks and the Customer Tax Integrity risks (hereinafter ML/ TF risks) faced by the bank. The steps to be taken are to:

- Identify the ML/ TF that are relevant to the bank;
- Assess the risks presented by:
  - the bank's particular customers and by any underlying ultimate beneficial owners (UBOs);
  - the products or services the bank offers;
  - the transactions the bank facilitates;
  - the delivery channels the bank employs (e.g. in person, through intermediaries, over the phone, online); and
  - the geographical areas in which the bank operates;
- Determine the bank's risk appetite based on the analysis of the above mentioned risks;
- Design and implement controls to manage and mitigate these risks, in accordance to 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 UBO, where appropriate.

1.1.2 Whatever approach is considered most appropriate to match the bank's exposure to ML/ TF risks, the broad objective is that the bank knows, at the outset of the relationship, who its customers (and, where relevant, UBO(s)) are, where they operate, what their main (professional) activities are, and is able to make a reasonable estimation of way in which the customer will engage with the bank (e.g. requested products and services including if applicable a picture of the expected transaction behaviour) are. The bank then must estimate how the customer's financial behaviour will change over time, thus allowing the bank to identify

unusual or even suspicious transactions or activities (hereinafter SAR).

1.2 Risk assessment

Wwft 2b

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 to, by taking into account:

- the information on ML/ TF risks made available to the banks by the supervisory authorities; and
- the 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 their business. Banks that do not offer complex products or services and that have limited or no international exposure may not need a complex or sophisticated business risk assessment.

Obligation to adopt a Risk-Based Approach

1.2.2 Senior management of most banks monitor a bank's affairs with regard to the risks inherent to its business, to its business environment and to the countries in which the bank operates, and the effectiveness of the controls they have put in place to manage these risks.

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

- Recognises that the ML/ TF threats to banks vary across customers, countries, products and delivery channels;
- Allows to differentiate between customers in a way that matches the risk of their particular business;
- Allows senior management to apply an approach that fits the bank's resources, capabilities, procedures, systems, controls, and arrangements in particular circumstances; and
- Helps produce a sustainable and effective AML/ CTF system.

Wwft 3(8),(9)

1.2.4 A bank uses its assessment of the risks inherent to its business to inform its risk-based approach to the identification and verification of each customer, which will in turn drive the level and the extent of due diligence appropriate to that customer.

1.2.5 No system of checks can detect and prevent all ML/ TF risks. A risk-based approach will however, serve to balance the cost burden placed on individual banks and on their customers, with a realistic assessment of the bank's exposure to ML/ TF risks. A risk-based approach helps a bank focus its efforts where they are needed and where they will have the highest impact.

1.2.6 The appropriate approach, in any given case, is a question of judgement, that senior management makes after considering the risks they determined that the bank faces.

1.3 Risk assessment – identification and assessment of business risks

Decree on Prudential Rules for Financial Undertakings 10, Wwft 2c(1)

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 performing a Systemic Integrity Risk Analysis (SIRA). Risk management is, in general, a continuous process, carried out on a dynamic basis.

Wwft 2c(1)

1.3.2 The European Commission (hereinafter EC)[12], the ESA (now: European Banking Authority (EBA))[13] as well as the Dutch government[14] publish risk assessment reports on ML/ TF, which provide a backdrop to a bank's assessment of the risks inherent to its business. Banks must use these publications as input, and must take account of relevant findings that affect their SIRA. The FATF publishes papers on the ML/ TF risks in various industry sectors (see www.fatf-gafi.org).

1.3.3 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 its business that are highlighted therein. Banks should be aware of the DNB's published enforcement findings in relation to individual financial institutions, and their actions in response to these.

Wwft 2b

1.3.4 The risk assessments carried out must be documented, kept up-to-date and made available to the DNB on request. The DNB

.....

[12] See EC "Anti-money laundering and counter terrorist financing", available at bit.ly/3d49JCr.
[13] See ESA "Joint Opinion on ML/ TF risks", available at bit.ly/3tM9d13.
[14] See WODC "Onderzoek in uitvoering", available at bit.ly/3tOip5Z.

may decide that a documented risk assessment, in the case of a particular bank, is not required when the risks inherent to the sector in which the bank operates are clear and well-understood.

1.3.5 The risk environment faced by the bank includes the wider context in which the bank operates, whether in terms of the risks posed by the countries in which it and its customers operate, the relative attractiveness (to criminals) of its products, or the nature of the transactions it facilitated. Among others, the extent to which a bank has, or has not, been able to carry out the appropriate level of CDD in relation to its customers/ UBO(s), the identity of the bank's customers and/ or of the UBO(s), and the activities undertaken by its customers (whether in relation to the bank or by using the bank's products and service, or through the transactions the bank facilitates), pose risks to the bank. A bank should therefore assess the risks it faces given how it could most likely be (mis)used for ML/ TF purposes. In this respect, senior management should ask themselves a number of questions; for example:

- What risks do the bank's customers pose?;
- What risks does a customer's behaviour pose?;
- How does the way the customer comes to the bank affect the risk?; and
- What risks do the products/ services the bank provides pose?

1.3.6 The business of many banks, their products and customer base, can be relatively simple – e.g. involving few products and with most customers falling into similar risk categories. In such circumstances, a less advanced approach (aligned to the risk the bank's products are assessed to present) may be appropriate for most customers, with the focus falling on the customers who do not fall in the defined risk categories. Other banks may have a wider range of business, and a large fraction of their customers may be retail customers, served through delivery channels that can have many standardized AML/ CTF procedures. Here too, the approach for most customers may be relatively straightforward, building on the product risk.

1.3.7 For banks that operate internationally, or that have customers based or operating abroad, there are additional risk considerations related to the aforementioned countries – such as their exposure to inherent ML/ TF risk, and the effectiveness of their AML/ CTF enforcement regime.

Delegated Regulation 2016/1675

1.3.8 The EC identifies high-risk third countries with strategic deficiencies in the AML/ CTF area.[15]

1.3.9 The ML/ TF risks associated with foreign countries may also be assessed using publicly available indices (e.g. the FATF high-risk and non-cooperative jurisdictions,[16] the FATF country evaluations, the OECD, the World Bank Governance Indicators,[17] and the Transparency International Corruption Perceptions Index[18]).

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

New technologies

Wwft 2a(2), FATF Recommendation 15; ESA ESA Joint Guidelines under Articles 17 and 18(4) of EU AML/ CTF Directive, Title II, paras 10, 32, 33

1.3.11 When identifying and assessing ML/ TF risks, banks must include the ML/ TF risks that may arise from (the development of) new products and new business practices (including new delivery mechanisms), and from the use of new or developing technologies for both new and pre-existing products. Apart from the specific requirement that banks must assess whether there is a high ML/ TF risk in a particular situation, this risk assessment should take place prior to the launch of the new products, of new business practices or prior to starting using new or developing technologies. Banks should take appropriate measures to manage and mitigate those risks, by including the application of enhanced due diligence measures where relevant.

1.4 A risk-based approach – Design and implement controls

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

1.4.1 Once the bank has identified and assessed the ML/ TF risks it faces, senior management must establish and maintain policies, controls and procedures to mitigate and manage effectively these risks.

1.4.2 The policies, controls and procedures refered to in paragraph 1.4.1 must take into account the size and nature of the bank's business. They should also be appropriate and proportionate to

.....

[15] See EC, EU policy on high-risk third countries, available at bit.ly/3rIsOhJ.
[16] See FATF, High-risk and other monitored jurisdictions, available at bit.ly/3rKdjGg.
[17] See World Bank, DataBank: Worldwide Governance Indicators, available at bit.ly/3d0l6LS.
[18] See Transparency Internation, Corruption Perception Index, available at bit.ly/3tOPZZO.

the aforementioned risks and should be designed to effectively mitigate them.

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

1.4.3 Senior management must approve the policies, controls and procedures referred to in paragraph 1.4.1. Senior management must also approve the monitoring and enhancing of any risk mitigating measures, where appropriate. In this context, senior management of a bank is defined as the persons who determine the day-to-day 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, that weaknesses are identified, and that improvements are made, wherever necessary.

1.4.5 The policies, controls and procedures referred to in paragraph 1.4.1 must include, but are not limited to:

- Risk management practices, customer due diligence, reporting, record-keeping, screening of staff, 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; and
- In case of a Group, the sharing of information about customers, customers accounts and transactions should be documented in a policy.

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; and
- The degree to which the bank outsources the operation of any procedures to other (Group) entities.

Wwft 3

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 UBO, and, with an appropriate degree of confidence, knows the types of business and transactions the customer is likely to undertake. The bank must have procedures to:

- Identify and to verify the identity of each customer on a timely basis before offering products and services;
- Identify the UBO and to take reasonable measures to verify that person's identity, so that the bank is satisfied that it knows who the UBO is (including that of legal persons, trusts and similar legal arrangements), by taking reasonable measures to understand the ownership and control structure of the customer;
- Assess and, when appropriate, to obtain information on the purpose and intended nature of the customer relationship;
- Conduct ongoing monitoring of the customer relationship. This should include the scrutiny of transactions undertaken throughout the course of that relationship, in order to ensure that the transactions conducted are consistent with the bank’s knowledge of the customer, the customer’s business and risk profile, including where necessary the source of funds.
- Ensure that documents, data or information held by the bank are kept up-to-date;
- Establish whether the natural person representing the customer is authorised to do so and, if applicable, to identify the natural person and to verify their identity;
- Take reasonable measures to verify whether the customer is acting on behalf of themselves or on behalf of a third party.

Wwft 2c(2)

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 is also 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-to-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, 3(8),(9)

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 UBO. It is likely that there will is a standard level of CDD that applies to the generality of customers, based on the bank's risk appetite.

ESA Joint Guidelines under Articles 17 and 18(4) of EU AML/ CTF Directive

1.5.2 Managing and mitigating the ML/ TF risks will involve measures to verify the customer's identity, collecting additional information about the customer, and monitoring their transactions and activity, to determine whether there are reasons to assume that transactions may involve ML/ TF. Part of the control framework involves 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 category of customer, customer relationship, product or transaction, geographies involved and distribution channel used.

1.5.3 To decide on the most appropriate and relevant controls for the bank, senior management must determine which measures the bank must adopt to manage and mitigate these threats/ risks

effectively. This must be in line with the bank's risk appetite. Examples of control procedures include:

- Introducing a customer identification program that is commensurate to the 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 the assessed ML/ TF risk; and
- Monitoring customer transactions and activities.

When assessing the extent to which each customer should be subject to each of these controls, it is important to the balance the controls and the risks the bank estimates for each individual customer, or category of customer to whom they belong.

1.5.4 A customer identification program that appropriately reflects risks 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 requirements (e.g. more identification checks and/ or requiring additional information) for 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 estimated for the customer, which will identify those transactions or activities that may be unusual or suspicious.

Customer risk assessment

Wwft 2b, 3(8)(9)

1.5.5 Although the ML/ TF risks that the bank faces 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 to the countries in which the bank and its customers operate. Banks should bear in mind that some countries have close links with other, perhaps higher-risk countries, 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 country with a reputation for ML/ TF, or in one which has a reputation for strong AML/ CTF enforcement, or whether a customer is resident in, established in or having its registered office in a high-risk country. 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 (mis)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 UBO, 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 start 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 started performing transactions 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 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 risks can be identified, of customers or categories of customers, and transactions allows banks to design and implement proportionate measures and controls to mitigate these risks.

ESA Joint Guidelines under Articles 17 and 18(4) of EU AML/ CTF Directive

1.5.12 Annex 1-II includes a more comprehensive 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 ESAs.

Wwft 2b, 3(9)

1.5.13 When assessing the ML/ TF risks relating to categories of customers, countries 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 (annex I of the EU AML/ CTF Directive):

- 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 EU AML/ CTF Directive, Ttile II, para 34

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

1.5.15 A risk assessment often results 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 EU AML/ CTF Directive, 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 – e.g., banks may decide that a customer's personal links to a country 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 their risk-weighting position. Parameters set by law or regulation may limit a bank's discretion.

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.

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 DNB, if necessary.

Risk assessment: Simplified CDD also known as adjusted CDD

EU AML/ CTF Directive 13(1), Annex II non-exhaustive list of factors of potential lower risks, Wwft 3(1)(2),6, 7, ESA guidance paper on risk factors paragraph 41 - 43

1.5.19 A bank's risk assessment must help it identify where it must focus its AML/ CTF risk management efforts, both at customer on-boarding and for the duration of the customer relationship. As

part of this, banks must apply the CDD measures as stated in 1.4.7.

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

1.5.21 Identifying a customer as carrying a higher ML/ TF risk does not automatically mean that they are 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 a money launderer or a financier of terrorism. Staff therefore need to be vigilant and use their experience and common sense in applying the bank's risk-based criteria and rules.

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

1.5.23 Banks must not, however, judge the level of risk solely on the nature of the customer or of the product. Before applying SDD, banks must demonstrate that the customer relationship is low risk further to a risk assessment of the customer. The information a bank obtains when applying SDD must enable the bank to be reasonably satisfied that its assessment that the low level of risk associated with the relationship, 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 EU AML/ CTF Directive para 45, Wwft 6, 7

1.5.24 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 UBO's identity during the establishment of the customer relationship; or
    - Verifying the customer's or UBO'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 UBO'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 lease 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 from an independent source when verifying the UBO(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 EU/ EEA Member State bank;

- Adjusting the frequency of CDD updates and reviews of the customer relationship, for example by 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 provided that there has been an adequate analysis of the ML/ TF risks relating to categories of customers, countries or geographic areas, and to particular products, services, transactions or delivery channels.

1.5.25 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. Also in case of SDD a bank needs to take reasonable measure to keep the data up-to-date and needs to ensure that ongoing monitoring of transactions is in place to detect unusual or suspicious transactions.

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

1.5.26 SDD does not exempt a bank from reporting SARs to the Financial Intelligence Unit (hereinafter FIU).

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

1.5.27 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, SDD must not be applied.

Risk assessment: Enhanced customer due diligence (hereinafter EDD)

Annex III non-exhaustive list of factors of potential higher risks of EU AML/ CTF Directive

1.5.28 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 (refer to 1.4.7). EDD means additional scrutiny or specific measures focused on risk factors that have been identified. Banks must assess identified risk factors 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.

At least the following situations are areas of higher-risk and therefore EDD must always be applied in case of:

- A higher ML/ TF risk;
- A customer resident in, established in or having its registered office in a high-risk third country identified by the EC;
- Complex or unusually large transactions or transactions that have no obvious economic or lawful purpose;
- Cross-border correspondent relationships involving the execution of payments (including but not limited to correspondent banks) established in non- EU/EAA Member States;
- A customer or a UBO is a Politically Exposed Person (hereinafter PEP).

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, established in, or having their registered office in geographical areas of higher-risk, as set out in point (3) below;
(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 and control structure of the company appears unusual or excessively complex given the nature of the company's business;
(g) Customer is a third country national who applies for residence rights or citizenship in the EU/EEA Member State in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities in that Member State.

Refer also to Annex 1-II.

(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 business relationships or transactions, without certain safeguards, such as electronic identification means, relevant trust services as defined in Regulation (EU) No 910/2014 or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities;
(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;
(f) Transactions related to oil, arms, precious metals, tobacco products, cultural artefacts and other items of archaeological, historical, cultural and religious importance, or of rare scientific value, as well as ivory and protected species.

Refer also to Annex 1-II.

(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 EU or the UN;
(d) Countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

Refer also to Annex 1-I.

Wwft 8

1.5.29 Banks must apply EDD measures in case the customer relationship or transaction by its very nature carries a higherML/ TF risk. 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[19];

.....

[19] Please note: Adopting a lower UBO threshold is only applicable for the bank. This will not affect the UBO-information in the UBO-register

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

1.5.30 Apart from the above mentioned, 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 in other high-risk situations it may be appropriate to focus on enhanced ongoing monitoring during the course of the customer relationship.

1.5.31 Banks must apply enhanced ongoing monitoring of both transactions and the risk associated with the customer relationship. Banks should identify SARs and regularly review the information they hold, in order 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.

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

1.5.32 Banks do 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, such as:
    i. Information about the customer's or UBO'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 UBO's reputation and assessing any negative allegations against the customer or UBO. Examples include:
        (a) Information about family members and close business partners;
        (b) Information about the customer's or UBO'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 create a more complete customer risk profile. This 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 suspicious deviations. 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 country;
    (c) The destination of funds; or
    (d) The nature of the customer's or UBO's business in order to better understand the likely nature of the customer relationship;

- Increasing the quality of information obtained for CDD purposes by:
    i. Requiring that the first payment be carried out through a verifiable account in the customer´s name, with a bank subject to CDD standards that are not less robust than those set out in the EU AML/ CTF Directive; 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. When 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 measures. 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 the bank is 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 in order to identify any unusual or unexpected transactions that may give rise to suspicions of ML/ TF. This may include establishing the destination of funds or ascertaining the reason for certain transactions.

Wwft 8

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

- Where a bank deals with a customer resident in, established in, or having their registered office in a country that has been designated by the EC as a country with higher ML/ TF risk;
- All complex or unusually large transactions, or unusual patterns of transactions, or transactions without an obvious economic or lawful purpose;
- Where a bank enters into a correspondent relationship involving the execution of payments with a respondent institution from a non-EU/EEA Member State;
- Where the customer or the UBO is a PEP.

In case of life insurance and other investment-related insurance policies, the verification of the identity of the beneficiaries shoud take place at the time of the payout. A bank must take reasonable measures to determine whether the beneficiary or the UBO(s) of the beneficiary of a life insurance policy is a PEP.

Politically Exposed Persons (PEP)

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

1.5.34 Banks must have in place appropriate risk management systems, including risk-based procedures, to determine whether the customer or the UBO of the customer is a PEP. In deciding whether a customer or the UBO of the customer is a PEP, the bank should take the list of the Dutch Ministry of Finance and the Ministry of Justice and Security into account.[20]

1.5.35 Banks can distinguish between a PEP as customer or PEP as UBO. If an UBO is identified as a PEP, the PEP's impact/ influence on the customer must be assessed and the intensity of the due diligence performed must be adjusted to mitigate the assessed risk.

Elements to be considered include whether:

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

1.5.36 Banks that have identified a PEP-customer or UBO 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 of corruption or of 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 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 when the risk associated with the PEP relationship is particularly high (refer to Annex 1-III for guidance on a risk-based EDD for PEPs);
- Obtain senior management approval for entering into, or continuing, a customer relationship with a PEP. Obtaining approval from senior management for establishing business

.....

[20] Refer to Belastingdienst "Politiek prominent persoon en de Wet ter voorkoming van witwassen", available at bit.ly/3tAuP0x. According to this list the Netherlands has no state-owned enterprises (hereinafter SOE), only state-participations (in Dutch *staatsdeelnemingen)*.

relationships does not need to imply, in all cases, obtaining approval from the person responsible for for the bank's compliance with the provisions of the Wwft. 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 the bank's risk exposure.

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

Wwft 8(7) and (8)

1.5.38 Banks must apply all of the above mentioned measures to PEPs, their family members and known close associates, and should adjust the extent of these measures in a risk-based way. If the customer or the UBO 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)

1.5.39 Banks must take specific EDD measures where they have correspondent relationships involving the execution of payments with a respondent institution from a non-EU/EEA Member State. Banks must apply all of these measures and must adjust the extent of these measures on a risk basis.

When entering into such a correspondent relationship a bank needs to:

- Gather sufficient information about the respondent institution to fully understand the nature of the respondent's business and to determine, from publicly available information, the reputation of the institution and the quality of the supervision it is subject to;
- Assess the respondent's AML/ CTF controls;
- Obtain approval from senior management before establishing the new correspondent relationship;
- Document the respective responsibilities of each institution;
- With respect to payable-through account, be satisfied that the respondent instution has verified the identity of,

and performend ongoing due diligenc on, the customers having direct access to accounts of the bank (the correspondent institution), and that the respondent institution is able to provide relevant cusomter due diligence data to the bank (the correspondent institution), upon request.

Please note that an increased ML/ TF risk could also arise in case of a correspondent relationship within the EU. In these situations, (a part of) the EDD-measures mentioned above apply.

High risk countries designated by the European Commission

Wwft 8(1), 9

1.5.40 When dealing with individuals or entities resident in, established in, or having their registered office in a high-risk third country identified by the EC, 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 increased monitoring, depends on the reason why a relationship is classified as high-risk.

1.5.41 Without prejudice to paragraph 1.5.39, the following EDD measures must be applied to occasional transactions or customer relationships with customers and respondent institutions that are resident in, established in, or have their registered office in high-risk countries (as identified by the EC):

- Obtaining additional information on these customers and on their UBO(s);
- Obtaining additional information on the purpose and the intended nature of the customer relationship;
- Obtaining information on the source of funds and source of wealth of these customers and of their UBO(s);
- Obtaining information on the reasons for the intended or performed transactions of these customers;
- Obtaining the approval of senior management for establishing or continuing the customer relationship; and
- Conducting enhanced monitoring of the customer relationship and of the transactions undertaken by these customers, by increasing the number and timing of controls applied and by selecting patterns of transactions that need further examination.

Complex or unusually large transactions or unusual patterns

Wwt 8(3)

1.5.42 Banks must have in place adequate policies and procedures to detect and examine transactions that fulfil one or more of the following conditions:

- 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;
- They have an unusual or an unexpected pattern compared to the customer's usual activity or to the transaction patterns associated with similar customers, products or services;
- They are complex compared to other, similar transactions by similar categories of customers, products or services;
- They do not have an apparent economic rationale or lawful purpose.

If one or more of these conditions are met, EDD measures must be applied and the degree and nature of the monitoring of the customer relationship needs to be increased. The intensity of the applied EDD measures and the monitoring of the customer relationship depends on the risk associated with the customer.

1.5.43 These EDD measures should help the bank to sufficiently and adequately determine whether these transactions give rise to suspicion of ML/ TF 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 by finding out more about the customer's business) in order to ascertain the likelihood of the customer making such transactions in good faith; 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 EU AML/ CTF Directive para 60

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

1.5.45 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 monitoring for standard CDD purposes:

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

Wwft 5(3)

1.5.46 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, suspend transactions, or take other risk mitigating measures, until it can be terminated. To prevent disruption of an ongoing criminal investigation, law enforcements authorities may require banks to suspend an intended termination of a customer relationship for a certain period. If this is the case banks must perform enhanced ongoing monitoring on this customer during this period.

1.5.47 If some situations are assessed as high-risk, or are outside the bank's risk appetite, the bank may wish to not take-on the customer, or may wish to terminate the relationship. This may be the case in relation to particular categories of customers, 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.

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

Wwft 16

1.5.49 Where, based on the above mentioned considerations, banks have reasonable grounds to suspect ML/ TF, they must report this to their FIU.

1.5.50 The application of a risk-based approach does not, in itself, require banks to refuse or to terminate customer relationships with entire categories of customers that they associate with

higher ML/ TF risk, as the risk associated with individual customer relationships may vary within a category of customers.

Wwft 3(2)

1.5.51 The bank must determine, on the basis of its assessment of the risks posed by different customer / product combinations, 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 has about a customer as this may alter the risk profile of the customer.

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

1. This annex is designed to assist banks by setting out how they might approach their assessment of other countries, to determine their level of ML/ TF risk. The annex discusses countries 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 country.

Implications of an assessment as low-risk

2. Assessing a country as low-risk only allows for some easement of the level of due diligence carried out. It does not exempt the bank from applying 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. It does not exempt the bank from reporting SARs.

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

Categories of country

(a) EU/EEA Member States

4. When identifying lower-risk countries, the 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/ CTF systems;
- Countries identified by credible sources as having a low-level of corruption or of other criminal activities.

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

5. All EU/EAA Member States are required to enforce legislation and financial sector procedures in accordance with the EU AML/ CTF Directive.

All EU/EEA Member States have undertaken to implement the EU AML/ CTF Directive and all are members of the FATF or of the relevant FATF-style regional body (e.g. in Europe this is MONEYVAL).

6. Given the commitment to implement the EU AML/ CTF Directive, banks may initially presume EU/EEA Member States to be low-risk; significant variations may however exist in the precise measures that have been taken to transpose the EU AML/ CTF 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, in order to take this information into account.

(b) FATF and FATF-style regional body members

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

8. However, unlike the transposition of the EU AML/ CTF Directive by EU/EAA Member States, implementation is not mandatory, and all members will approach their obligations in different ways, and follow different timetables.

9. Information on the effectiveness of the implementation in these countries may be obtained through scrutiny of Mutual Evaluation reports, which are published on the FATF website[21], as well as through the FATF public statements and the DNB newsletters[22]. Whenever banks have substantive information indicating that a presumption of low-risk cannot be sustained, either in general or for particular products, they need to consider whether to enhance their procedures 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.[23] 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 through 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

.....

[21] FATF website, available at www.fatf-gafi.org.
[22] DNB, News, available at www.dnb.nl/en/actueel/dnb.
[23] OECD, Council Recommendations, available at bit.ly/3jYhWtw.

Recommendations. Whenever banks have substantive information indicating that a presumption of low-risk cannot be sustained, either in general or for particular products, they need to consider whether to enhance their procedures to take this information into account.

(d) Other countries

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

Factors to consider when assessing other countries

13. Factors include:

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

Geographical risk factors

14. Geographical risk factors include:

- Countries identified by the EC as having strategic deficiencies in their national AML/ CTF regimes, that pose significant threats to the financial system of the Union ('high-risk third countries) based on article 9 of the EU AML/ CTF Directive;
- Countries identified by credible sources (e.g. the (FATF) mutual evaluations, detailed assessment reports or published follow-up reports) as not having effective systems to counter ML/ TF;
- Countries identified by credible sources as having significant levels of corruption or of other criminal activity (e.g. terrorism, money laundering 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 UN;
- 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 EU as terrorist organisations.

The presence of one or more risk factors may not always indicate that there is a high ML/ TF risk in a particular situation.

Membership in an international or regional 'group'

15. There are a number of international and regional 'groups' of countries that admit as members only those countries that have demonstrated a commitment to fighting against ML/ TF and which have an appropriate legal and regulatory regime to back up this commitment.

Contextual factors

16. Factors such as the political stability of a country, and where it stands in corruption rankings are relevant to determine whether a country is low-risk. Since it is seldom easy for the bank to make this assessment, it may rely on external agencies for gathering the evidence – whether prepared for general consumption, or specifically for the bank. When the bank uses publicly available evidence, it should have some knowledge of the criteria used to make the assessment. The bank cannot rely solely on an existing independently prepared assessment, even if prepared by a respected third party agency.

Evidence of relevant (public) criticism

17. From time to time the FATF issues statements on its concerns about the lack of comprehensive AML/ CTF systems in a number of countries (see section 2.4 below). When constructing their internal procedures, therefore, all 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.

18. Furthermore, other commercial agencies also produce reports and lists of countries, 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 or lists can provide useful and relevant evidence, which may or may not be conclusive, on whether or not a particular country is likely to be low-risk.

Mutual evaluation reports

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

FATF

20. FATF member countries monitor each other's progress in the fight against ML/ TF through regular mutual evaluation. In 1998, the FATF extended the concept of mutual evaluation beyond its own membership by endorsing FATF-style mutual evaluation programs 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);[24]
- The Caribbean Financial Action Task Force (CFATF);[25]
- The Asia/Pacific Group on Money Laundering (APG);[26]
- MONEYVAL, Council of Europe countries that are not FATF members;[27]
- The Financial Action Task Force on Money Laundering of Latin America (GAFILAT);[28]
- The Middle East and North Africa Financial Action Task Force (MENAFATF);[29]
- The Eurasian Group (EAG);[30]
- The Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG);[31]
- The Intergovernmental Action Group against Money-Laundering in West Africa (GIABA).[32]

21. 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 country. Even at the time of the evaluation there can be changes to the country'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 country is low-risk.

22. Summaries of FATF and FATF-style evaluations are published in FATF Annual Reports.[33] Mutual evaluation reports prepared by some FATF-style regional bodies may not be fully carried out to the FATF standards, and banks should consider this when their decision to view a country as low-risk is based on such reports.

.....

[24] Offshore Group of Banking Supervisors, available at www.ogbs.net.
[25] Caribbean Financial Action Task Force, available at www.cfatf.org.
[26] Asia/Pacific Group on Money Laundering, available at www.apgml.org.
[27] Council of Europe, Moneyval, available at www.coe.int/Moneyval.
[28] Financial Action Task Force on Money Laundering in South America, available at http://www.gafilat.org/.
[29] Middle East and North Africa Financial Action Task Force, available at www.menafatf.org.
[30] Eurasian Group, available at www.eurasiangroup.org.
[31] Eastern and Southern Africa Anti-Money Laundering Group, available at www.esaamlg.org.
[32] Intergovernmental Action Group against Money-Laundering in West Africa, available at www.giaba.org.
[33] FATF, Annual Reports, available at www.fatf-gafi.org.

IMF/ World bank

23. As part of their financial stability assessments of countries and territories, the IMF and the World Bank have agreed with the FATF on a detailed methodology for assessing compliance with AML/ CTF standards, based on the FATF Recommendations. A number of countries have already undergone IMF / World Bank assessments in addition to those carried out by the FATF, and some of the results are available on the IMF website[34]. 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)

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

Advisory notices

FATF

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

26. The FATF issues two public documents periodically:

    1. The first public document, the statement "*High-Risk Jurisdictions subject to a Call for Action*", indentifies countries with serious strategic deficiencies to counter money laundering, terrorist financing and financing of proliferation.[35] For all countries identified as high-risk, the FATF calls on all members and urges all countries to apply enhanced due, and in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the ongoing money laundering, terrorist financing, and proliferation financing risks emanating from these countries.
    2. The statement "*Jurisdictions under Increased Monitoring*" identifies countries that are actively working with the FATF to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing.[36] When the FATF places a country under increased monitoring, it means that the country has committed to resolve the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring.

.....

[34] See International Monetary Fund, Anti-Money Laundering/ Combating the Financing of Terrorism Assessments, available at bit.ly/3qvPnpA.

[35] This is often referred to as the FATF "black list".

[36] This is often referred to as the FATF "grey list".

DNB/ European Central Bank (hereinafter ECB)

27. Supervisory authorities (incl. DNB/ ECB) expect banks to keep abreast of revisions of the FATF Statements and to consider the impact of these statements when assessing country risks.

Factors to be taken into account when assessing non-transparant countries

28. The following factors may be taken into account when assessing non-transparent countries:

a. The country is identified by the IMF as an Offshore Financial Centre;[37]
b. The country is identified by the OECD[38] as a country committed to improving transparency and establishing an effective exchange of information in tax matters.
c. The country is identified by the EU as a third country for tax purposes;[39]
d. The country is identified by the Dutch Ministry of Finance.[40]

Other countries might be added to the list of non-transparent countries based on the banks' internal analysis.

.....
[37] See IMF, *Past IMF Staff Assessments on Offshore Financial Centers*, available at bit.ly/37pnAjf.
[38] See OECD, *Jurisdictions committed to improving transparency and establishing effective exchange of information in tax matters*, available at bit.ly/3ptlOmj.
[39] See European Commission, *Common EU list of third country jurisdictions for tax purposes*, available at bit.ly/3dm6hDn.
[40] See Rijksoverheid, *Nederland stelt zelf lijst laagbelastende landen vast in strijd tegen belastingontwijking*, available at bit.ly/2NcXKbe.

Annex 1-II Illustrative risk factors relating to customer situations

Note: These are risk factors that may be relevant for consideration during the course of risk assessments but do not automatically indicate a higher risk.

I. Risk Factors related to the Customer

A. Business or professional activity

Questions that may be worth asking when considering the risk associated with a customer's or with their UBO's business or professional activity include:

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

- Does the customer or the UBO have links to sectors and/or industries 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 PEP, or is their UBO a PEP? In which country is the PEP, their business, or the business that they are connected with, located?

- Does the customer or UBO 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 public contracts, or 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 UBO is publicly available, for example public companies listed on stock exchanges that make such disclosure a condition for listing?

- Is the customer a credit or financial institution from a country with an effective AML/ CTF regime and is it supervised on their 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 in recent years?

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

- Is the customer's or their UBO'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 UBO's source of wealth (if applicable)?

- Is the customer a beneficiary of a life insurance policy (that the bank has become aware of) in situations where there may be an increased risk, for example complex products with potential multiple investment accounts or those that allow for early surrender and have a surrender value, or beneficiaries with no obvious links to the policy holder?

- Is the customer a third country national who is applying for residence rights in or citizenship of an EU/EEA Member State in exchange for transfers of capital, purchase of property, government bonds, or investment in corporate entities in that EU/EEA Member State?[41]

B. Reputation

The following questions may be worth asking when the bank considers the risk associated with a customer's or with their UBO's reputation:

- Are there any adverse media 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 UBO(s)? 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 on the basis of 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, their UBO(s), 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 their UBO(s) have been subject to a SAR in the past?

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

C. Nature and behaviour

The questions listed below may be worth asking when the bank considers the risk associated with a customer's or with their UBO'(s) nature and behaviour. Not all of these

.....

[41] see also Annex III - List of high risk sectors

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 their identity, perhaps because they are an asylum seeker?

- Does the bank have any doubts about the veracity or accuracy of the customer's or of the UBO'(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, does it have no physical presence (other than a mailing address) and does it generate little or no independent economic value?

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

- 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 that 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 reporting 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 UBO'(s) source of wealth or source of funds be easily explained, for example, by their occupation, by an inheritance or by their investments?

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

- Where the customer is a non-resident customer, 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? EU law creates a right for private individual consumers who are legally resident in the EU and have a economic interest in The Netherlands to obtain a basic bank account. This right applies however, only in sofar as the bank can comply with their AML/ CTF obligations.

- Is the customer a non-profit organisation whose activities expose it to high TF risks?

II. Risk Factors related to Countries and Geographic Areas

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

(a) The country where the customer or their UBO(s) reside in, are established in, or have their registered office in;
(b) The countries where the customer´s or their UBO'(s) main place of business is; and
(c) The country to which the customer or their UBO(s) has relevant links.

Annex 2-I further guides banks on what to take into consideration when assessing the level of ML/ TF risk in different countries.

III. Risk Factors related to Products, Services and Transactions

When identifying the risk associated with their products, services or with transactions they facilitated, 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.

Questions that may be worth asking when considering the risk associated with the transparency of a product, service or transaction include:

- To what extent do products or services facilitate or allow anonymity or opacity of the customer, of ownership or beneficiary structures (e.g. 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; 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 relationships)?

Questions that may be worth asking when the bank considers the risk associated with the complexity of a product, service or transaction include:

- To what extent is the transaction complex and does it involve multiple parties or

multiple countries (e.g. certain trade finance transactions)? Are transactions straightforward (e.g. 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 (e.g. 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 EU AML/ CTF Directive?

- 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?

Questions that may be worth asking when the bank considers the risk associated with the vale or size of a product, service or transaction 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 that could limit the use of the product or service for ML/ TF purposes?

- Is there a transaction "related to"[42] oil, arms, precious metals, tobacco products, cultural artefacts, ivory and other items related to protected species, or to other items of archaeological, historical, cultural and religious significance, or of rare scientific value, where the ML/ TF risk is raised? See below.

Banks should consider all relevant information at their disposal concerning ML/ TF risks arising from transactions listed in Annex III of the EU AML/ CTF Directive and should consider their exposure to potential high-risk transactions involving these items, as identified through undertaking risk-based CDD measures on their customers.

A "transaction" involves two parties who are making or benefiting from the transaction, or executing it (the customer and the bank), and includes a bank facilitating a transaction between two third parties.

Transactions should be considered on a risk basis in all instances. The below mentioned examples of scope are not exhaustive:

Oil: Transactions made to and/or from parties in the oil production process, including the sale of oil to exploration companies and refiners. Banks should consider terrorist financing methodologies. Retail customers purchasing refined oil products from petrol retailers should not be included.

.....

[42] A risk-based approach should be adopted in the interpretation of "related to" in this context. Banks should consider the closeness of the relationship or link between the item and the transaction, as well as between the transaction and the customer and/ or bank.

See also FATF Reports:

- Emerging Terrorist Financing Risks[43]
- Specific Risk Factors in Laundering the Proceeds of Corruption[44]

Arms: Transactions such as those relating to a trade in live firearms or customers involved in the arms trade should be considered.

Precious metals: Transactions involving large/medium scale industrial miners to/from PEPs should be considered, as well as those made by refineries to their suppliers and wholesalers or vice versa. EDD should be considered on transactions involving gold recyclers and jewellers on a risk basis.[45]

Tobacco Products: Transactions involving wholesalers and their suppliers rather than retail sale of tobacco to the public should be considered, as well as identified risks such as “boot legging”.[46]

Cultural artefacts or other items of archaeological, historical, cultural or religious significance, or of rare scientific value: Banks should adopt definitions of these items considering Annex 1 of the EU’s 2019/880 Regulation on the Import of Cultural Goods[47] and consider the ML/ TF risks identified in the EU’s 2019 Supra National Risk Assessment.[48] This includes the looting and trafficking of antiquities and other artefacts.

Ivory or other items related to protected species: Banks should consider the Convention on International Trade in Endangered Species of Wild Fauna and Flora (hereinafter CITES) definitions of ivory and other protected species. EDD should be performed on transactions involves CITES items on a risk basis of potential illegal wildlife trafficking (hereinafter IWT). IWT can mean the domestic or international trade of CITES species in contravention of national or international laws.

Specific considerations could include:

- In-/ out-bound transactions involving zoos, pet stores involved in the sales of animals, safari companies, hunting reserves or timber importers. Large deposits/ withdrawals from government officials who work in environment or other related government departments that have oversight of government stockpiles of seized ivory, rhino horn, timber, or those working in forestry agencies, wildlife management authorities, or CITES Management Authorities.
- Transactions involving Asian nationals operating import/ export, international trading, or transport companies in Africa and suspected of transporting CITES products.

Examples of transactions involving traders who may sell CITES products indirectly, and are not subject to EDD include: cosmetic retailers who may sell products containing fragments of orchid or cacti; food retailers who may sell products containing caviar

.....

[43] FATF (2015) *Emerging Terrorist Financing Risks*, available at bit.ly/2Zy4PWl.
[44] FATF (2012) *Specific Risk Factors in Laundering the Proceeds of Corruption*, available at bit.ly/2M0SIhv.
[45] FATF (2015) *Money laundering / terrorist financing risks and vulnerabilities associated with gold*, available at bit.ly/2ZpnzHN.
[46] FATF (2012), *Illicit Tobacco Trade,* available at bit.ly/2NhhL0r.
[47] Regulation (EU) 2019/880 on the introduction and the import of cultural goods, available at bit.ly/2LZJT7C.
[48] EC (2019) *Supranational risk assessment of the money laundering and terrorist financing risks affecting the Union*, available at bit.ly/2OFKIDy.

extract; musical instrument manufacturers who may sell products containing rosewood or ivory.

IV. Risk Factors related to the Delivery Channel

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 the latter's relationship to the bank.

The bank may rely on certain third parties for the following CDD measures:

- 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.

Questions that may be worth asking when the bank assesses the risk associated with the way the customer obtains their products or services, include:

- 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 bank used an electronic identification process that is fraud- and misuse-proof or able to provide an appropriate level of assurance?

- 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 domestic 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 the provision of financial services? What has the bank done to be satisfied that:

  (I) The third party applies CDD measures and keeps records, in line with domestic standards, and that it is supervised for compliance with comparable AML/ CTF obligations, in line with domestic requirements?
  (II) The third party will provide, immediately, upon request, among others, relevant copies of identification and verification data, in line with domestic 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?

Questions that may be worth asking when the bank uses an intermediary, include:

(I) Is the intermediary a regulated person subject to AML/ CTF obligations that are consistent with those as layed down in the EU AML/ CTF Directive?

(II) Is the intermediary subject to effective AML/ CTF supervision? Are there any indications that the intermediary's level of compliance with applicable AML/ CTF legislation or regulation is inadequate, for example because the intermediary has been sanctioned for breaches of AML/ CTF obligations?

(III) Is the intermediary based in a country 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 domestic requirements.

Annex 1-III Considerations in the treatment of politically exposed persons for AML purposes

Banks apply a risk-based approach to identifying PEPs, be it a customer or an UBO of a customer. A PEP is always a natural person and must be subject to enhanced due diligence measures. The legislation and guidance clarify that the risk assessment of individual PEPs should take place on a case-by-case basis rather than through a generic approach to all PEPs. The EDD measures that banks take depend on the level of risk associated with the customer relationship. The extent of the EDD measures must be adjusted on a risk basis.[49]

Once a bank is satisfied that a PEP is a UBO 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 risk mitigating measures. This could range from enforcing applicable EDD 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), to enforcing applicable EDD measures (according to the risk assessed) when it is apparent the PEP has effective control over the entity or has the ability to use their own funds in relation to the entity.

Even if a customer meets the definition of PEP (because of the position they hold), a bank may decide to recognise the lower risk of the PEP customer. For example, the risk associated with a domestic PEP opening an account to manage their daily household finances may differ from the risk associated with a foreign PEP requiring private banking services. The intensity of EDD measures can be adjusted to the specific circumstances. For example, obtaining approval from senior management[50] for establishing customer relationships does not need to imply, in all cases, obtaining approval from the board of directors or from 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 the bank’s risk exposure.[51]

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 about the proposed customer relationship. This is in line with the regulatory guidance to date, where the focus has been on managing higher

.....

[49] ESA Joint Guidelines under Articles 17 and 18(4) Directive (EU) 2015/849.

[50] 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 private individuals whose activities influence the exposure of a bank to the risks of ML/ TF (see articles 1(1) and 8(5)(a)(1) Wwft).

[51] Directive 2015/849, preambule, para 34.

risk PEP relationships. This is because FATF Recommendations recognise that a PEP may be in a position to abuse their public office for private gain and that 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'.[52]

The measures banks should take to establish the PEP's source of wealth and the source of funds also depend on the degree of high-risk associated with the customer relationship. 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, of family members or of known close associates of a PEP – e.g. by verifying information through open sources or by only use information already available to the bank (such as transaction records or publicly available information) and by not making 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 (e.g. via information sources it has available). Where the risk associated with the PEP relationship is particularly high, banks must verify the source of wealth and the source of funds on the basis of reliable and independent data, documents or information (refer for examples of documentation to the table at the end of this annex). In cases where it proves impossible to establish the source of wealth, the bank must be able to demonstrate that it has taken sufficient effort to discover the source of wealth.

The following indicators suggest that a PEP poses a lower risk:

Lower-risk factors – product:

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

Lower-risk factors – geographical:

- A PEP who is entrusted with a domestic prominent public function should be treated as lower 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 Factor Guidelines issued by the ESAs 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;
    - Credible AML defences;
    - A free press with a track record for probing official misconduct;

.....

[52] FATF (2013) *Politically Exposed Persons*, available at bit.ly/3s52gHD.

- 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 factors – personal and professional:
A PEP may pose a lower risk if they:

- Are subject to rigorous disclosures requirements (e.g. 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).

The following indicators suggest that a PEP poses a higher risk:

Higher-risk factors – geographical:
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 crime;
- 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 factors – personal and professional
The following characteristics might suggest a PEP is higher risk:

- 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 (e.g. facilitated, made or accepted bribes);
- Is responsible 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 licences (e.g. mineral extraction concessions or permission for significant construction projects).

A family member or close associate of a PEP may pose a lower risk if also the PEP poses a lower risk. Banks may expect family or known close associates of domestic PEPs to be treated as lower risk, unless there are circumstances to suggest otherwise.

The following characteristics might suggest a family member or a close associates of a PEP poses a higher risk:

- Wealth derived from the granting of government licences (e.g. 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 with 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 (e.g. 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:

- Seek to make no inquiries into a PEP's family or known close associates, except those necessary to establish whether such a relationship does exist;
- Take less intrusive and less exhaustive steps to establish the source of wealth and source of funds of PEPs and of their family members or known close associates of a PEP (e.g. 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 that the bank seeks the 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 the efforts put into verifying the information provided (e.g. by using only information sources it has available).

In higher-risk situations a bank may take more intrusive and more exhaustive steps to establish the source of wealth and source of funds of PEPs and of their family members or known close associates.

Annex 1-IV 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; • Recent copy of annual income tax declaration.
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 was it 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 was it sold (i.e. through agent, by auction, private sale, incl. name/ address); • Date of sale; • How long property held.	• Signed letter from solicitor; • Completed sale contract.
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;	• Grant of probate (with a copy of the will) which must include the value of the estate;

	•Date received.	•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 source of wealth 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 1-V Considerations in keeping risk assessments up-to-date

Banks should keep their assessment of ML/ TF risk associated with individual customer relationships and with 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 their earlier 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 in their 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 to 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 countries 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 by looking for sanctions regime updates; and
    - Regularly reviewing thematic reports and similar publications issued by supervisory authorities.

- Processes to capture and review information on risks relating to new products or services;

- Engagement with other industry representatives and with supervisory authorities (e.g. round tables, conferences and training) and processes to feed back any findings to the relevant staff; and

- Establishing a culture of information sharing within the bank and a 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 1st of 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 SAR, 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: 2.1.3 – 2.1.10
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 (introduction and outsourcing) : 2.6
Monitoring customer activity: 2.7

Wwft 2b

2.1.2 Banks must determine the extent of their CDD measures and ongoing monitoring on a risk basis, depending on the category of customers, customer relationships, products or transactions, geographies involved and distribution channel used. 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 ML/ TF risks.

What is customer due diligence?

Wwft 3

2.1.3 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 of each UBO and that it knows, with an appropriate degree of confidence, the types of business and transactions the customer is likely to undertake. The bank must have procedures to:

- Identify and verify the identity of each customer, on a timely basis, before offering them products and services;
- Identify the UBO and takes reasonable measures to verify that person's identity so that the bank is satisfied that it knows who the UBO is (incl. as regards to legal persons, trusts and similar legal arrangements) and takes reasonable measures to understand the ownership and the control structure of the customer;
- Assesses and, when appropriate, obtains information on the purpose and intended nature of the customer relationship;

- Conducts ongoing monitoring of the customer relationship including scrutiny of transactions undertaken throughout the course of that relationship, in order to ensure that the transactions being conducted are consistent with the bank's knowledge of the customer, the business and risk profile of the customer (incl., where necessary, the source of funds) and in order to ensure that the documents, data or information held are kept up-to-date;
- Establishes whether the natural person representing the customer is authorised to do so and, if applicable, identifies the natural person and verifies their identity;
- Takes reasonable measures to verify whether the customer is acting on behalf of themselves or on behalf of a third party.

2.1.4 Where the customer is a legal person (other than a Recognised Exchange listed entity), trust or similar legal arrangement, banks must take reasonable measures to understand the ownership and the control structure of that legal person, trust or similar legal arrangement.

2.1.5 Working out who an UBO is may not be a straightforward matter. Different rules may apply to different forms of entity (see section 2.5 below).

Wwft 6, 7, 8, 9

2.1.6 For some customer relationships, determined by the bank to present a low ML/ TF risk, SDD may be applied.[53] In the case of higher-risk situations, in the case of transactions or relationships with customers resident in, established in, or having their registered office in high-risk countries identified by the bank or the EU Commission, in the case of PEPs or of correspondent relationships with non-EU/EEA respondents, banks must enforce EDD measures on a risk-based approach.[54]

What is ongoing monitoring?

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

2.1.7 Banks must conduct ongoing monitoring of the customer, including the scrutiny of transactions undertaken throughout the course of the relationship and must keep CDD information up-to-date. This is a related obligation, but it is separate from the requirement to apply CDD measures. CDD information is updated when relevant circumstances of a customer change, or when there is any legal duty to contact the customer for the purpose of reviewing any relevant information relating to their

.....

[53] For Guidance on applying SDD refer to paragraphs 1.5.19 – 1.5.27.
[54] For Guidance on applying EDD refer to paragraphs 1.5.28 – 1.5.51.

UBO(s), or when the bank has this duty under the Common Reporting Standard.[55] Banks must consider whether information received as a result of any of these obligations contains changes that require CDD measures to be applied on a risk-based approach. Refer also to paragraph 2.3.48.

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

2.1.8 Banks need to know who their customers are, in order to prevent that they are (mis)used for ML/ TF purposes. For this reason, banks apply (amongst other) CDD measures and conduct ongoing monitoring.

2.1.9 More specifically, the bank needs to carry out CDD and must conduct ongoing monitoring in order to:

- Be, at the time CDD is carried out, reasonably satisfied that customers are who they say they are, know whether the customers are acting on behalf of themselves, and know that there is no legal barrier (e.g. government sanctions) that prevents the bank from providing them with the products or services requested; and
- Report SARs.

2.1.10 It may be appropriate for the bank to know more about the customer than their identity. The bank should, for example, be aware of the nature of the customer's business or activities, in order to assess the extent to which their transactions and activity (undertaken with or through the bank) are consistent with the customer's business.

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

Wwft 3(5)

2.2.1 A bank must apply CDD measures when:

(a) It establishes a customer relationship;
(b) It carries out an occasional transaction on behalf of a customer amounting to € 15.000 or more (whether the transaction is executed in a single operation or in several operations which appear to be linked);
(c) It has indications that the customer is involved in ML/ TF;
(d) It doubts the veracity of documents or information previously obtained for the purpose of identification and verification of the customer's or (if applicable) of the UBO'(s) identity;

.....

[55] Council Directive 2011/16/EU of 15 February 2011, on administrative cooperation in the field of taxation.

(e) The risk of a customer being involved in ML/ TF gives rise thereto;
(f) It identifies a higher ML/ TF risk, based on the country in which the customer is resident, established, or in which the customer has their registered office; or
(g) It carries out a transaction on behalf of a customer or trust, as defined in article 3 (9) of Regulation (EU) 2015/847, that exceeds € 1.000.

Timing of verification

Wwft 4(1),(3),(4)(6)

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

2.2.3 **Exception**: The verification of the identity of the customer, and (if applicable) of the UBO(s), 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,

provided that verification is completed as soon as practicable, after the first contact with the customer.

When this exception is applied for the opening of an account, the verification of the identity of a customer (or UBO(s), if applicable) may take place after the account (incl. an account which permits transactions in transferable securities) has been opened, provided that there are adequate safeguards in place to ensure that no transaction is 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), the bank is allowed to establish the identity of the beneficiary at the time the payment is made or when the beneficiary excersises their vested rights. The bank is only allowed to do so, if before entering into the customer relationship or before executing the transaction, the beneficiary is defined according to specific characteristics or by category, and if the bank obtains sufficient information to establish the identify of the beneficiary at the time the payment is made, or when the beneficiary excersises its vested rights

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.

To ensure that banks are able to terminate an existing customer relationship adequately, the bank needs to have an ‘exit policy’. The exit policy should give guidance under which circumstances and through which process(es) banks can terminate a customer relationship.

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 ML/ TF suspicion, 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 appropriate mitigating measures.

Electronic transfer of funds

EU 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 EU/EEA Member States. It requires payment services providers (hereinafter PSPs) to include certain information in electronic funds transfers and to 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. There are, however, a number of permitted exemptions, concessions and variations. Adequate CDD measures will support banks to meet these requirements of Regulation 2015/847.

2.2.10 The Regulation 2015/847 includes (among others) the following definitions:

- 'Payer' means a person that holds a payment account and that 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 (PSP)' means a natural or legal person (as defined) providing transfer of funds services;
- 'Intermediary PSP' means a PSP that is not the PSP of the payer or of the payee, and that receives and transmits funds on behalf of the PSP of the payer or of the payee, or of another intermediate PSP.

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, of UBO(s), including other relevant related parties. 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

2.3.2 A "customer relationship" is defined in the Wwft as a business, professional or commercial relationship between a bank and a natural person, legal person or partnership, connected to the professional activities of the bank, and is expected by the bank to have an element of duration at the time when contact is established. 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 component with a ML/ TF risk, the Wwft is applicable to these activities as well. An example is transactions for telecom-companies (related to text or to '0900'-services) that are provided by PSPs. This means that relationships with professional counterparties in the context of the core activities of the bank, such as relationships with financial institutions and with financial

service providers, fall under the definition of correspondent relationships.

A relationship does not require bank involvement in an actual transaction – e.g. giving advice may 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 exceeding €1,000 within the meaning of Regulation (EU) 2015/847; or
- A transaction performed outside the context 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 – e.g. 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 is the party, or parties, with whom the customer relationship is established, or for whom or on whose behalf the transaction is carried out. When, however, there are several parties to a transaction, not all are necessarily customers or relevant related parties. Refer to part II of the NVB AML, CTF & Sanctions Guidance for more information on when a certain party in a transaction should be considered a customer of the bank (e.g. Chapter 8 Corporate Finance, Chapter 9 Trade Finance).

Wwft 3, 11, 33

2.3.6 The bank identifies the customer by obtaining a range of information about the customer. The verification of the identity consists of the bank verifying this information against documents, data or information obtained from a reliable source which is independent from the customer. Providing services to anonymous customers (e.g. any anonymous accounts, or anonymous safe-deposit boxes) 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 of the similar legal arrangement; and
- The governing law by which the trust or the similar legal arrangement is governed.

Developments in identification and verification

ESA Opinion on the use of innovative solutions by credit and financial insitutions when complying with their CDD obligations; Regulation (EU) 910/2014

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 - e.g. eIDAS[56] electronic identification (eID) means, or eIDAS trust services or solutions that have similar levels of assurance as eIDAS notified schemes. The application of remote (digital) verification of identity must be in line with applicable regulatory requirements and be demonstrably reliable and appropriate. 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, and to assess the extent to which the use of innovative technological solutions can affect the ML/ TF risks, in particular in non-face-to-face situations.

This includes the assessment of:

- Whether there is a substantial or high-level of assurance (which is the degree of confidence that can be put in the claimed identity of a person) with any electronic ID system used;
- Whether the provider keeps all necessary documentation, information and data received as part of the CDD process. Following regulatory request, the bank must be able to provide copies of records held without delay;
- Whether the bank has appropriate technical skills to oversee the development of methods of digital verification and the proper implementation of these innovative solutions, particularly where activities are outsourced to a third party;
- Whether senior management and compliance officer(s) have a proper understanding of the innovative solution;
- Whether the bank has proper contingency plans in place. The continuity of the provision of services needs to be guaranteed

.....

[56] Regulation (EU) 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, available at bit.ly/3bhp2pa.

in case of system failures, or when the cooperation with the provider comes to an end;

- Whether there are qualitative risks, in particular the risk that the sources used for verification purposes are not sufficiently independent and reliable, and the risk that the level of identity verification provided by the innovative solution does not correspond with the level of ML/ TF risk associated with the customer relationship;
- Whether there are technical risks, in particular the risk that the innovative solution may be unreliable or could be tampered with;
- Whether there are legal risks, in particular the risk that the provider does not comply with privacy and with the applicable data protection legislation;
- Whether there are impersonation fraud (i.e. that a customer is not the person who they claim to be) risks. The bank should also consider the risk that a person does not exist. The use of biometric data can be a possible control. Where customers are required to give their approval, consideration should be given to the possibility that the customer may prevent the access to certain information to conceal certain facts.

Based on the results of the assessment, as mentioned above, the bank should conclude whether the innovative technological solution is within the bank's ML/ TF risk appetite.

The assessment, including the risk factors mentioned above, are further elaborated and made more concrete 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*"[57] and in ESA The Risk Factor Guidelines (specifically regarding criteria when using an external provider).[58]

Non-face-to-face verification of the identity

EU AML/ CTF Directive Annex III, part (c)

2.3.9 According to EU AML/ CTF Directive Annex III non-face-to-face customer relationships or transactions, without certain safeguards (e.g. electronic identifications means, relevant trust services as

.....

[57] EBA (2018) *ESAs publish Opinion on the use of innovative solutions in the customer due diligence process*, available at bit.ly/3s7Mmwb.

[58] See paragraphs 4.34 and 4.35 of EBA (2020) *Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions,* available at bit.ly/3aAjVkC.

defined in Regulation (EU) No 910/2014,[59] or any other secure, remote or electronic identification process regulated, recognised, approved, or accepted by the relevant national authorities) are considered to be of potentially higher risk.

ESA Joint Guidelines under Articles 17 and 18(4) of EU AML/ CTF Directive items 32

2.3.10 Delivery Channel Risk is the extent to which the customer relationship is conducted on a non-face-to-face basis where no adequate additional safeguards (as referred to in paragraph 2.3.9) are in place. In such cases, identification and verification take place within the risk framework of a remote customer. Non-face-to-face customer relationships or transactions, without certain safeguards, present a potentially higher risk. Therefore, it is necessary to take additional risk-based measures to mitigate this risk.

EDD measures in relation to non-face-to-face verification of the identity

EU AML/ CTF Directive 18-24, ESA ESA Joint Guidelines under Articles 17 and 18(4) of EU AML/ CTF Directive items 32 and 49

2.3.11 When identifying the risk associated with the way in which customers obtain the products or services they require, banks must 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, questions worth asking include:

- Has the bank used a reliable form of non-face-to-face identity verification?
- Has the banktaken steps to prevent impersonation or identity fraud?

2.3.12 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.

Wwft 8(2), 11(1)

2.3.13 The following EDD measures may be considered:

- Verifying the identity of the customer on the basis of additional documents, data and information that have been submitted (refer to paragraphs 2.3.15 and 2.3.16);

.....

[59] 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 EU.

- Assessing the authenticity of the documents (refer to paragraph 2.3.17);
- Ensuring that the first payment related to the customer relationship or transaction, is credited to or debited from a customer's account held with a financial institution holding a valid licence, and supervised by a regulator registered on the Recognised Regulators List. Also referred to as derived verification (refer to paragraph 2.3.18).

These measures are in themselves not sufficient to verify the identity of the customer. A bank must determine on the basis of its own risk assessment which combination of additional measures, documents and information is adequate to verify the identity of a customer in a non-face-to-face situation.

2.3.14 *Additional documents, data and information*
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. The 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, that are independent from the customer.[60] These are the well-known and accepted identity documents, as referred to in article 4(1) of the Wwft Implementing Regulation (refer also to section 2.4). 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 may serve as additional verification, but cannot be used on their own:

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

.....
[60] See Wwft, art. 11.

2.3.15 As far as a document is needed, an original or a copy can be requested. An original provides more certainty that the information is correct, but requesting original documents is more difficult for both the bank and the customer. If the documents do not come from public authorities or from judicial authorities, the bank may question whether the documents are sufficiently reliable. Such documents will, in themselves, often be insufficient to adequately verify the identity, but they can serve as additional information. Documents from a regulated sector can, in principle, be regarded as relatively reliable. Documents from another source or documents that are easily obtainable without certainty that adequate identification and verification have preceded it (e.g. student cards, employee cards, (some) foreign driving licences (without photo)), are, in themselves, not sufficient to verify the identity.

2.3.16 *Assess the authenticity of the 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. What matters is that the identity of the customer being established and verified. Ways for banks to check the authenticity of documents include (but are not limited to):

- Checking internal and external systems (e.g. EVA, SFH and VIS), in line with the bank's risk-based approach;
- Making use of external parties that can check the security features of the identity documents;
- Verifying by means of the original identity document (to be returned to the customer by the bank);
- A statement or note on the document of an independent third party that the document is genuine;
- New technology on remote verification of the identity without certain safeguards[61] such as the use of digital identity like iDin.

2.3.17 *Derived verification of the identity*
In the case of derived verification of the identity, verification of the identity of the customer takes place by making use of the identification previously collected by a licenced financial institution from an EU/EEA Member State. With this form of verification, it is important that there is sufficient certainty that the

.....
[61] Examples of new technology on remote verification of the identity with certain safeguards are relevant trust services as defined in Regulation (EU) No 910/2014 and secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities.

customer has identified themselves elsewhere, and that in this way they can be traced via an audit trail.

This form of verification means that the bank ensures that the first payment related to the customer relationship or to 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 on the basis of 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, in order to ensure adequate identification.

2.3.18 *Other EDD measures in relation to non-face-to-face verification*
The above mentioned measures are non-exhaustive. Banks can take other measures to identify and verify the identity of non-face-to-face customers. Finally banks have to be comfortable that the measures are sufficiently adequate.

Identification and verification of an UBO

2.3.19 An UBO is an individual who ultimately owns or controls the customer or on whose behalf a transaction is being conducted.

Wwft 3 (2) f

2.3.20 Private individuals are usually also the UBOs, unless there are features of the transaction, or surrounding circumstances, that indicate otherwise. Therefore, there is no requirement for banks to do proactive searches for UBOs in such cases. Banks should, however, make appropriate inquiries where it appears that the customer is not acting on their own behalf. Where a private individual customer, is a straw man that is fronting for another individual who is the UBO, the bank must obtain the same information about that UBO as it would for the customer.

Wwft 3a

2.3.21 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 (e.g. ‘children’), then the bank obtains sufficient information regarding the UBO to be satisfied

that at the time of payment, the identity of the UBO can be established. Verification of the identity of the UBO takes place when the life insurance policy pays out. If a life insurance policy is transferred to the bank, the bank shall identify the UBO at the time of the transfer to the private individual, legal entity or legal arrangement that will receive the value of the transferred policy for their own benefit.

2.3.22 The UBO(s) must always be identified and the bank must take reasonable measures to verify their identity.

2.3.23 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 residence;
- Size and nature of the UBO capacity (through ownership and/or control).

2.3.24 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 UBO.

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

2.3.25 The obligation to verify the identity of an UBO means that the bank must take reasonable measures such that it is satisfied that it knows who the UBO is. It is up to each bank to consider whether it is appropriate, in the light of the ML/ TF risk associated with the customer relationship, to make use of records of UBOs from the public domain, to ask the customer for relevant data, or to require evidence of the UBO's identity on the basis of documents, data or information obtained from a reliable source, independent from the customer.

2.3.26 In general it may be reasonable for the bank to confirm the identity of the UBO(s) based on information supplied by the customer. This could include information provided by the customer (incl. trustees or other representatives whose identities have been verified) as to their identity, and the confirmation that they are known to the customer. While this may be provided orally or in writing, the bank should record in writing any information it received orally.

Thereafter, the bank must take reasonable measures to verify the information supplied by the customer. The manner and depth of the verification process is risk-based, and can be done by using public sources, an extract from the Trade Register of the Chamber of Commerce (hereinafter Trade Register), or a confirmation of an independent third party. When entering into a new customer relationship with a legal person, banks must determine whether the UBO(s) are registered in the UBO register. Evidence of registration of the UBO(s) in the UBO register must be obtained before entering into a new customer relationship.

The obligation to consult the UBO register applies when entering into a new customer relationship. During ongoing monitoring banks may discover a change in UBO(s) of an existing customer. In those cases, it is reasonable that banks also consult the UBO register to determine whether these newly identified UBO(s) correspond to the UBOs registered in the UBO register. The obligation to report discrepancies applies when discrepancies are identified both for new and existing customers.

2.3.27 In case of higher risk of misrepresentation, the use of a statement from the customer (e.g. a self-declaration form) is not sufficient and additional documentation and information from (other) reliable -and based on the risk involved independent- sources, is required. Banks could request additional relevant documents from the customer that, depending on the risks involved, may be verified by an independent third party or through other sources.

Wwft 10c (1)(3), 3(15)

2.3.28 Banks may not exclusively rely on UBO-information registered by the customer in the public UBO-register. There may be situations when the bank, based on its knowledge of the customer and of their organisational 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 this case, the bank must report the identified discrepancy to the Chamber of Commerce as soon as reasonable possible after the discrepancy has been established. In case the established discrepancy gives reason to report to the FIU, the reporting duty to the Chamber of Commerce is not applicable.

A discrepancy report to the Chamber of Commerce is not a substitute for a SAR and the requirement to submit a SAR to the FIU, where appropriate, remains. Discrepancies should have a certain level of materiality to be reportable. A discrepancy itself

does not prohibit the onboarding of a customer. Instead, the nature and relevance of the discrepancy should be assessed by the bank, based on their CDD process and on their risk-based approach during onboarding, and considering whether there are reasonable grounds for suspicion.

Existing customers

2.3.29 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 specific additional products or services or establishing a new relationship, might prompt a bank to seek appropriate evidence.

2.3.30 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 by the bank, than approaching customers for more identification data or information.

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

2.3.31 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 of that other financial institution 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 when a portfolio of customers or business has been acquired, that the identities of its customers were verified.

2.3.32 It is however, important that the acquiring bank's due diligence inquiries 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 the Dutch AML/ CTF requirements.

2.3.33 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 in line with the requirements for existing customers opening new accounts.

Purpose and intended nature of the customer relationship

Wwft 3(2)(c)

2.3.34 A bank must understand the purpose and intended nature of the customer relationship or transaction, in order to assess whether the (future) customer relationship is in line with the bank's expectation, and in order 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.

Part of the required information can be obtained during contact with the customer prior to the establishment of the customer relationship. The purpose of the relationship can also be apparent from the services or products used by the customer.

For customers that are not resident in, established in, or having their registered office in the country where the bank is operating its services from (i.e. non-resident customers), the bank should establish why the customer intends to use its services or products from that location. If that is for tax purposes, for example, the bank should assess the acceptability of that purpose. Refer to Chapter 7.

2.3.35 By gathering this information the bank must assess any risks that may arise from the provision of services to the customer. See also section 1.5 above.

2.3.36 Purpose and nature inquiries establish, to the extent applicable and required, what type of transactions the customer intends to perform (e.g. number, frequency and size of transactions).

Banks should thoroughly analyse the answers of the customer regarding purpose and nature of the relationship. 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 this concern arises, the bank should consider terminating the relationship. applicable).

2.3.37 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. A customer's situation may change after onboarding and during the customer relationship.

Wwft 8 (1)(b)

2.3.38 When assessing the ML/ TF risks related to customer categories, countries or geographic areas, 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[62] (see 1.5.19 – 1.5.51). These variables, on their own or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Refer to Chapter 1.

Source of funds and source of wealth

Guidance regarding the source of funds and the source of wealth

2.3.39 *Defining source of funds and source of wealth*
The difference between source of funds and source of wealth can be explained as follows:

- *Source of funds* refers to 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 (e.g. the customer's salary), as well as the means through which the customer's funds were transferred.

- *Source of wealth* refers to the origin of the customer's or of the UBO'(s) total wealth (e.g. inheritance or savings).

Legal requirements and industry standards

Wwft 3(2)(d)

2.3.40 A bank must establish, where needed, the source of the funds that will be used in the relationship or transaction on a risk-based

.....
[62] Ibid 58.

approach. A bank must document this assessment. Where necessary, the bank must record statements, must document evidence in customer files, and must ask further questions. In high-risk situations, banks should determine and record the plausibility of the funds using reliable sources (refer to Annex 1-IV for examples).

To determine the plausibility that the funds originate from a legitimate source, the bank must identify specific indicators that determine the depth of the review. The bank can consider combinations of indicators (e.g. the amount involved, the reason given for the source of funds, the business activities of the customer, the country of origin or the 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, banks should, especially in the case of high-risk customers, 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.

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

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

2.3.42 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 is plausible, must be assessed in the light of all risk factors identified in relation to a particular customer relationship or in relation ot an occasional transaction. A bank must therefore perform EDD in case a customer relationship or a transaction, by its nature or in relation to the country where the customer resides, is established or has its registered office, poses a higher ML/ TF riskML/ TF. Certain combinations of risk factors may lead to EDD, and if necessary, to the verification of the origin of the assets.

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

2.3.43 A bank must monitor transactions to ensure that they are in line with the customer's risk profile and with the 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 of crime. The level of due diligence will depend on

the degree of 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 that emerge during the customer relationship include:

- 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 that 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 reporting thresholds (e.g. those described in Article 11(b) of the EU AML/ CTF Directive 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;
- The customer engages in transactions designed primarily to generate a tax benefit. Refer to Chapter 7.

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 of 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.

DNB Guidance on the AML/ CTF Act and Sanctions Act section 4.7

2.3.44 The plausibility of the source of funds used in the customer relationship or in the occasional 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 when monitoring a customer relationship. If necessary, the bank must 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 proportional to the risk identified.

Elements the banks should consider are:

- Whether the source of funds is in line with the overall customer profile (i.e. purpose and nature of the customer relationship);
- Whether the source of funds is plausible, based on the statements of the customer;
- Whether the source of funds is plausible on the basis of other sources (e.g. 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 more difficult to verify on the basis of public sources, if the assets were entered into the bank account more than five years ago;
    - The more time has passed since the assets were acquired, the bank may accept more limited information.

2.3.45 In situations where there is doubt about the information provided or where there are certain red flags, further due diligence may be required. The bank must be wary of over-reliance on customer explanations and vague responses should be clarified and/or challenged. The plausibility of the source of funds and/ or assets should then be determined based on independent and 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 (e.g. in case of private banking customers).

Wwft 8(5), ESA Joint Guidelines under Articles 17 and 18(4) of EU AML/ CTF Directive, Title II

2.3.46 Banks that have identified that a customer or an UBO 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 of crime. The measures banks must take to establish the PEP's source of funds and the source of wealth depend on the degree of risk associated with the customer relationship. Banks must verify the source of funds and the source of wealth on the basis of reliable and, when the risk

associated with the PEP is particularly high, on the basis of independent data, documents or information.

If the customer or the UBO becomes or proves to be a PEP in the course of the customer relationship, the bank must take additional measures, as quickly as possible. The bank must take these measures on a risk-based approach, recognizing that establishing the source of wealth of an UBO who is a PEP can be difficult in some situations. When it is impossible to establish the source of wealth, the bank can demonstrate that it has made sufficient effort to establish it.

If the PEP has an 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.

Refer to Annex 1-III for more guidance on the assessement of the source of funds and source of wealth relating to PEPs.

Keeping information up-to-date

EU AML/ CTF Directive 28(11)(b), Wwft 3(11)

2.3.47 Documents, data and information obtained and held by the bank for the purpose of applying CDD measures must be kept up-to-date. A bank needs to take reasonable measures to keep up-to-date information about:

a) the customer;
b) the UBO(s); and
c) the authorised representatives of the customer.

The risk profile of the customer must also be kept up-to-date. The higher the risk, the more often the CDD data must be updated.

Once the identity of a customer has been verified, there is no obligation to re-verify their identity (unless doubts arise as to the veracity or adequacy of the evidence previously obtained for this purpose). Moreover, a range of events (e.g. an existing customer requesting a specific additional product or service or establishing a new relationship) might prompt the bank to seek appropriate evidence. See also to paragraph 2.1.7.

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. This section provides further guidance on steps that may be applied as part of a risk-based approach.

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. Otherwise, assessments based on unverified data may yield faulty conclusions. 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 A clear distinction must be made between identification and the verification of identity:

- *Identification* means that the bank obtains the first name(s), surname, address and date of birth, either from the customer themselves or from a third party (free of form);
- *Verification* means that the bank establishes that the customer details are correct, based on data, documentation and information from a reliable source and that is independent from the customer. The sources used may vary, in line with the bank's risk-based approach.

Identification

Wwft 33(2)(a)

2.4.4 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 from the customer, and can be obtained in various ways. In respect of private individuals, much weight is placed on so-called 'identity documents' (e.g. passports). For verification purposes, the use of (certified copies of) identity documents prevails.

There is no legal obligation to keep a copy of the identity document, if the bank records the needed information arising from the identity document.

2.4.6 It is however possible to have a reasonable belief as to a customer's identity, based on other methods of verification. These can be different types of documents but also information and electronic/ digital data held by various organisations. These documents, information and data vary in terms of 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.). Banks should use a risk -based approach (taking into account all inherent ML/ TF risk factors) to determine how much identity documentation, data and information is needed in order to have a reasonable belief as to a customer's identityML/ TF.

Customers who cannot provide the standard evidence

2.4.7 Where a bank concludes that a private individual customer cannot reasonably meet the standard identification requirements,[63] it may accept as identification evidence a letter or a statement from a reliable source who knows the individual, and that indicates that the customer is who they say they are. Alternative methods can be used to verify the person's identity.

Directive (EU) 2014/92

2.4.8 In the Netherlands[64] every adult needs an own payment account to be able to participate in society. Banks and social work

.....

[63] EBA (2016) *Opinion of the EBA on the application of customer due diligence measures to customers who are asylum seekers from higher-risk third countries or territories*, available at bit.ly/3qB9hje.

[64] 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 as until 2016 there was no statutory right to a

agencies have therefore agreed that everyone in the Netherlands over 18 years of age, with a known address, must be able to open a (basic) payment account. In 2001 the 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 Documentary evidence of an individual's identity that provides a high-level confidence, is typically issued by a government department or agency, or by a court or (local) public authority, that has checked the existence and the characteristics of the individual concerned. When such documentary evidence is not be available, banks should consider if other documentary evidence is sufficiently reliable and could give the bank reasonable confidence in the customer's identity. Alternative verification methods should be included in the banks risk assessment. Refer to section 2.3.

Implementation Regulation Wwft4 (1)

Article 4(1) of the Implementation Regulation Wwft mentions the following non-exhaustive list of documents with a high-level of conficence:

- A valid passport;
- A valid Dutch identity card;
- A valid identity card issued by the competent authority in an EU/EEA Member State, and bearing a passport photo and the name of the holder;
- A valid Dutch driving licence;
- A valid driving licence issued by the competent authority in an EU/EEA 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;
- A sufficiently reliable identification method. This means a method with certain safeguards (e.g. electronic identification means, relevant trust services as defined in Regulation (EU) No 910/2014, or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities).

.....

basic payment account in the Netherlands, as there has been for most EU citizens since then (see Basisbankrekening, Wat is een basis-bankrekening, available at bit.ly/3bhYtQI).

Banks should recognise that some documents are more easily forged or counterfeited than others. If suspicions are raised in relation to any document, banks should take practical and proportionate steps to establish whether the document has been reported as lost or stolen. Consideration should be given to an increased risk of forgery or counterfeiting of paper documents, as customer statements can be indistinguishable from originals.

Other considerations

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

Wwft 3 (2e) (2f)

2.4.10 If the customer is represented by a private individual, the Wwft requires that this representative is identified and that their identity is verified. The bank also needs to determine whether the relevant person is authorised to represent the customer. The bank can do so by obtaining a copy of the document describing the powers of the person(s) acting towards the bank (e.g. a written power of attorney from the customer or a court order). This is not required for a legal representative of a minor.

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

- Parent or guardian.[65] Once a customer becomes authorised to represent themselves (e.g. a minor becoming an adult) the identity of the customer must be verified;
- Representative appointed by court order (i.e. curator/ “bewindvoerder”);
- Notarial Attorney[66] (i.e. “notarieel gevolmachtigde”);
- Representative authorised otherwise by the private individual to act on their behalf.

Wwft 33 (2a)

2.4.11 The bank must indentify any representative of a customer (private individual) who acts on the customer’s behalf and must verify their identity as if they were a customer. The bank must record in the customer file the same data for the representative as for the private individual customer they represent (as detailed in paragraphs 2.4.4 to 2.4.9).

.....

[65] Guardianship is the custody of minor children that is not exercised by the parents, but by someone else, in the form of the guardian. This can be either a natural person or a legal entity (guardianship institution).

[66] 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.

Minors

2.4.12 Often a customer relationship in respect of a minor is established by a parent or by a guardian. When the adult opening the account or establishing the relationship does not already have an existing relationship with the bank, the bank must verify the identity of that adult,[67] unless the bank strongly suspects that the person is not the parent.

In the latter case, the bank must request a copy of the birth register or of the Marriage Act. The bank may also ask the adult for an up-to-date extract from the authority register (gezagsregister). The bank must then verify, in person, the identity of the minor with their own identity card, once the minor becomes authorised to represent themselves.

2.4.13 The identification and verification of the minor customer can take place in two ways:

1. The minor appears in person with their own identity document. The bank must also idenfy and verify the identity of the parent or guardian;
2. The parent or the guardian identify and verify the minor using the identity document of the parent or guardian.

In the second case, the verification of the identity has a limited shelf life: the minor will have to have their identity verified in person, with their own identity card, once they become authorised to represent themselves.

2.5 Entities (i.e. customers other than private individuals)

2.5.1 Depending on the nature of the entity, a relationship or transaction with a customer who is an entity (i.e. not a private individual), may be entered into in the customer's own name, or in that of specific private individuals, or of other entities, on their behalf. Beneficial ownership may, however, rest with others, either because the legal owner is acting for the UBO, or because there is a legal obligation for the ownership to be registered in a particular way.

.....

[67] For parents/ legal representatives of minor customers, it is sufficient to provide personal data of the minor combined with an explicit declaration by the parent that as parent and legal representative they are authorised to represent the minor.

2.5.2 This section provides guidance on identifying and verifying the identity of the following types 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, such as:
    - General partnerships (in Dutch *vennootschap onder firma (VOF)*);
    - Professional partnerships (in Dutch *maatschap*);
    - Limited partnerships (in Dutch *commanditaire vennootschap (CV)*); and
- Trusts and similair legal arrangements.

2.5.3 Banks may take a risk-based approach when determining the extent of the CDD measures. Some of the types of entities listed above may entail a lower ML/TF risk. If the risks associated with them are low, SDD may be applied. Refer to paragraphs 1.5.19 to 1.5.27.

Wwft 33 (2) sub c

2.5.4 Banks must record the following details for entity customers:

- Full legal name;
- Trading name(s) where applicable;
- Legal form;
- Proof of existence;
- Registered address or legal seat in country of incorporation or organisation (incl. 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 the company legal identification number, if there is no registration number at the Chamber of Commerce); and
- The representatives of the customer and their:
    i) Full name; and
    ii) Date of birth.

Wwft 11(2)(3)

The information must be verified based on documents, data 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.

Implementation Regulation of the Wwft 4(2)

2.5.5 Banks can use the following (non-limitative) list of sources:

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 EU/ EEA 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.

2.5.6 Registration in the Dutch Trade Register 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.

2.5.7 Information relating to foreign legal entities can (also) be obtained through the Trade Register in the country of incorporationor 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, a bank can consult reports from authoritative international organisations, such as the Financial Action Task Force.

Wwft 8(5), 9(1)

2.5.8 If an entity is known to be linked to a PEP (i.e. the PEP being a UBO of the entity), or to a country assessed as carrying a higher ML /TF risk, enhanced due diligence measures must be applied

Identification and verification of the UBO

2.5.9 When deciding who the UBO is, in relation to an entity customer, the bank’s objective must be to know who has ownership or control over the funds. Verifying the identity of the UBO(s) will be

carried out on a risk-based manner and will take into account the number of individuals, the nature and distribution of their interests in the entity, and the nature and extent of any business, or contractual or family relationship between them. Refer to paragraphs 2.3.19 – 2.3.28.

Identification of effective control

2.5.10 Apart from the UBO(s) that have an ownership interest or control, there may be situations where non-identified individuals may exercise effective control over the customer through other means, and therefore, qualify as UBOs.
The FATF gives the following description of effective control:

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 (e.g. shareholders' 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 (incl. 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 private individual(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 private individual(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 (e.g. 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 other UBO(s) have effective control.

Understanding the ownership and control structure

Legal requirements and industry standards

WWft 3(2)(b)

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

Section 4.5 DNB Guidance on the AML/ CTF Act and the Sanctions Act

2.5.12 Banks must 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 private individuals, if possible, by obtaining proof of incorporation. Banks must know the relevant structure and must understand it. 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 it does for a Dutch private limited company (or in Dutch *besloten vennootschap* hereinafter BV) with a majority shareholder-director. As part of these efforts, the bank examines the customer's reasons for using complex structures. The bank can achieve this by inquiring of the customer, or by requiring a legal or a tax opinion/ advice. Gaining insights into the customer's fiscal motives, in the context of customer due diligence, enables the bank to determine whether there are any tax integrity risks. The examination into the customer's ownership and control structure is closely related to the purpose and nature of the relationship and to the assessment of customer tax integrity risks (see Chapter 7).

ESAs Guidelines on risk factors – Customer risk factors

2.5.13 A factor that may contribute to increasing the risk level is when the customer's UBO cannot be easily identified -e.g. 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

2.5.14 Therefore, an EDD measure that may be appropriate in high-risk situations, ensures that the bank is satisfied that its customer uses complex business structures (e.g. trusts and private

investment vehicles) for legitimate and genuine purposes only, and that the identity of the UBO is established.

FATF Guidance on Transparency and Beneficial Ownership

2.5.15 For example, UBO 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 countries;
- Complex ownership and control structures involving many layers of shares, which are 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 (e.g. close associates and family);
- Trusts and other legal arrangements that enable a separation of legal ownership and of beneficial ownership of assets;
- Use of intermediaries in forming legal persons (incl. professional intermediaries).

Identification of complex structures

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

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

2.5.18 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.

2.5.19 A complex structure in itself does not necessarily indicate ML/TF. The reasons for complex structures may be legitimate and could

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 and/or to facilitate tax evasion. Refer to Chapter 7.

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

- A structure consisting of more than four 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 four layers are not considered complex in case all the criteria below are met:
  - All intermediate parent companies are incorporated in the same country (low and medium risk countries only) as the customer;
  - The UBOs are resident in the same country as the customer;
  - There are no complex entities in the structure;
  - The structure matches the profile of the customer; and
  - No other red flags for complex structures are present.
- The structure contains companies that have been incorporated in non-transparant countries;
- Knowledge of presence of bearer shares and of 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 UBO is undisclosed.

2.5.21 EDD on complex structures will not be required for Recognised Exchange listed entities, for Recognised Regulated entities and for more than 75% state-owned enterprises, if no other red flags have been identified regarding the ownership and control structure, and where the level and nature of complexity is assessed as being proportionate and explicable.

2.5.22 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.

EDD measures for complex structures and effective control

2.5.23 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 independent and reliable sources;
- Identification of the immediate and intermediate parents and risk-based verification of their legal existence through independent and reliable sources;
- Assessment of the rationale provided by the customer for 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. Refer to Chapter 7.

Specific measures apply for the following situations:

2.5.24 *Shell companies and non-transparent countries.*
Ownership and control structures involving non-transparent countries require EDD measures due to the increased risk of tax evasion and of obscuring the trail to the UBO(s). 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 should 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 obtain insight into the structure “underneath” as the source of funds may be from complex structures.

2.5.25 *Bearer shares*
Banks may establish a relationship with customers, in whose structure bearer shares have been identified, if the holders of all outstanding shares are identified by means of:

- Converting them into registered shares (e.g. through dematerialisation); or
- Immobilising them, by requiring them to be held in custody with a Recognised Regulated entity or with a professional intermediary regulated by a Recognised Regulator.The bank must receive an official statement from the custodian stating the details of the UBO(s) holding the shares and verify their

identity. The custodian must also state that it will immediately inform the bank of any change in ownership, or in case the shares are withdrawn from custody.

The requirements above 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 UBO(s); and
- Verify whether local applicable laws require private individuals owning more than 10% of the shares to notify the company to record their identity, and the company to inform the bank immediately of any change in ownership.

The Financial Secrecy Index (Tax Justice Network, 2020) Interactive Database[68] may serve as starting point in researching the legal provisions (e.g. acceptance of bearer shares without registration, phasing out of anonymous bearer shares, etc.) surrounding bearer shares world wideworldwide.

2.5.26 Complex entities in the structure
An ownership structure involving complex entities will require different EDD approaches, depending on the type of entity. The definition of a UBO may differ for each of these entities (see paragraphs 2.3.19 – 2.3.28).

2.5.27 *(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 UBO(s) 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

.....
[68] Use of the TJN, Financial Secrecy Index Interactive Database (available at bit.ly/2NRQrpl) should be done subject to licence terms and conditions.

third parties, the bank should obtain, at least, the following information and documents:

- 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 the 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 from the UBO(s).

(ii) In case the customer makes use of *nominee directors*, the bank should obtain, at least, the following information and documents:

- A statement from the service provider with the details of all proxy holders and their powers;
- A 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 *case another legal entity is appointed as director*, the bank should obtain, at least, the following information and documents:

- The power of attorney of the private individuals that represent the legal entity directly or indirectly, in the capacity of director of the customer;
- A justification from the customer, for the use of such a structure, in case the legal entity director again has a legal entity as director.

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

Identification and verification of representative(s)

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

2.5.28 Customers, other than private individuals, are represented by one or more private individuals. Banks should take appropriate steps to be reasonably satisfied and be confident that the private individual they are dealing with is properly authorised to represent the customer. The adequate representation must be

established and verified, for reasons of transparency and to prevent ML/TF risks. Misrepresentation is a legal risk and it may constitute a fraud risk. Therefore, the bank must establish, by using reliable sources (e.g. power of attorney), whether:

- The private individual representing the customer currently has a formal role with that entity (i.e. has been duly appointed and has not been discharged); and
- Tn that role, the private individual may face the bank on behalf of the entity.

2.5.29 Where a private individual claims to indirectly represent an entity, the chain of representative authority needs to be established.

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

2.5.30 Banks must verify the identity of authorised private individuals based on reliable and independent documentation, data or information. The nature and the extent of the information required for identification and verification depends on the risks involved (incl. the customer category, the nature of the relationship, the product or the transaction). See also section 2.4.

2.5.31 There are the following categories of authorised representatives:

1. *Direct appointees/ authorised representatives by force of law:* These private individuals represent the customer towards the bank at a customer-relationship level, in general, and are legally authorised by statutory provision, articles of association, or by relevant law. Examples include: company directors, the company secretary, the trustee, the managing partners, etc.
2. *Authorised representatives by proxy:* These private individuals 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: Examples include: authorised signatories, proxy holders, holders of power of attorney, etc.

2.5.32 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 private individual to represent the customer and the verification of their identity may take place as part of the product process. The bank should take care that relevant documentation is available in the CDD file of the customer. Banks do not have to re-establish this information during a regular CCD-review, but should process updates on an event driven review (e.g. renewal of a loan agreement).

Section 4.2.2 DNB Guidance on the AML/ CTF Act and Sanctions Act

2.5.33 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 have a procedure in place to establish who represents the customer and to verify whether these persons are authorised by the entity to do so. This can be established without verification of identity of those private individuals. In those circumstances, it is sufficient for the bank to establish the capacity of those private individuals 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 private individuals are a.o. the use of a (bank) card, (PIN) code, or a specimen of the authorised signature provided by the entity. The bank may decide on a risk-based approach to screen these persons against sanctions and applicable internal lists.

2.5.34 The Wwft does not specify how banks should examine whether the representative is duly authorised to represent the customer, except that banks may determine the extent of such measures on a risk-based approach. This means that depending on the circumstances, independent and reliant sources are used in determining an authorised representative's power to represent. A bank needs to determine how it complies with this obligation. In practice, this means that banks have to request a power of attorney, or check the Trade Register. 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

2.5.35 As part of their risk-based approach, banks should consider recording one or more directors for screening purposes.

Corporate entities

2.5.36 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 on other regulated markets, and are subject to market regulation and to high levels of public disclosure in relation to their ownership and to their business activities. Other public companies are unlisted, but are still subject to high levels 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 process, banks should take account of the availability of public information in respect of different types of company.

2.5.37 A public limited company (or in Dutch *naamloze vennootschap,* hereinafter NV)), is a company whose capital is divided into shares, in a similar way to that of a 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.

2.5.38 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 banks need to take, to be reasonably satisfied as to their identities. The use of complex ownership structures does not necessarily indicate ML/TF. Nevertheless, the use of complex structures without an obvious legitimate commercial purpose may give rise to concern, and may increase the ML/ TF risks. Refer to paragraph 2.5.23 - 2.5.27.

2.5.39 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 evaluate the effective distribution of control in each case. What constitutes control, for this purpose, depends on the nature of the company, the distribution of shareholdings (refer to paragraph 2.5.71 - 2.5.73 for more information regarding Stichting Administratiekantoor, hereinafter STAK), on and the nature and extent of any business or family connections between the UBOs.

2.5.40 The bank takes 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 on the reasons for seeking the product or service.

Wwft 3(2)b, Implementing Decree Wwft 2018, 3

2.5.41 In case of a public limited company (whose share are not traded on a recognised stock exchange), a limited company or a similar legal entity, the following private individual is defined as an UBO:

1. Private individual who is the beneficial owner of or has control over the legal entity via:

a. The (in)direct holding of more than 25% of the shares of the legal entitity;
b. The (in)direct holding of more than 25% of the voting rights; or
c. The (in)direct holding of more than 25% of the ownership interest;

2. Private individuals who otherwise exercise effective control over the customer, based on the responsibility for the strategic decisions that fundamentally affect the daily or the regular affairs/ business of the customer; or
3. If the situations described in points 1. or 2. are not applicable, and when there are no grounds for suspicion that there is an UBO as defined in points 1. or 2., all private individuals who hold the position of senior managing official; or
4. If there is uncertainty whether the individual(s) identifified is, in fact, an UBO, all private individuals who hold the position of senior managing official.

2.5.42 Identifying senior managing officials as UBOs can only be done as a last resort, when there are no grounds for suspicions and in case of doubt. In case senior managing officials qualify as UBOs, the reasoning for designating these persons as UBOs should also be recorded.

2.5.43 Normally, if an UBO is established for a customer 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 company(ies) that is 100% owned by the customer. This is only in sofar as there are no indications that the operating company has another UBO(s). However, if the senior managing official is identified as an UBO because no UBO could be identified under the definition as stated in paragraph 2.5.41, 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(s).

2.5.44 Banks may adopt a lower threshold than the more than 25% stated in 2.5.41 in cases that present a high risk to the bank. This is particularly the case if the bank is not reasonably satisfied that it knows who the UBO(s) is (e.g. 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). If the bank adopts a lower UBO threshold in

high-risk cases, there can be a difference between the UBO(s) identified by the bank and the UBO(s) identified in the UBO register.

2.5.45 In order to verify the director or the 100% shareholder of a corporate as the UBO, the bank can use an extract from the Trade Register which states the name of the director or of the 100%-shareholder.

Corporate entities listed on a Recognised Exchange

EU AML/CTF Directive

2.5.46 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 to their business activities. Therefore, these customer relationships may present a low degree of ML/TF risk and SDD measures may be applied (refer to Annex II to EU AML/CTF Directive). In determining whether a customer relationship presents a lower ML/TF risk and therefore whether SDD 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 if it is an 100%-owned subsidiary of such a listed company (refer to Anex I List of Recognised Exchanges); and
- Carry-out a risk assessment of 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 1.5.19 - 1.5.27 for more information on SDD.

2.5.47 If the bank establishes 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.

Implementing Decree Wwft 2018 3(1)(a)

2.5.48 If the customer is a company listed on a Recognised Exchange, there is an exemption under law to identify and verify the UBO(s). Given the fact that there is no legal obligation to identify the

UBO(s) 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 direct or an indirect 100% subsidiary of a company listed on a Recognised Exchange. The UBO exemption is also applicable to a subsidiary that is 50% owned by company A and 50% owned by company B AND both company A and company B are listed on a Recognized Exchange. Based on the risks involved, the bank may decide not to apply the exemption and to identify and verify the UBO(s).

2.5.49 In more developed markets, in general, the bank can expect fragmented ownership in the case of listed companies on a Recognised Exchange. However, in less developed markets the ownership might not be as fragmented e.g. in the case of family-owned entities where family members do not sell out, or in the case of family-owned entities where family members are in the process of selling out over time. In these or in similar cases, it is best practice that the bank describes the ownership- and control structure of these companies even when why are listed on a Recognised Exchange.

Regulated credit and financial institutions

FATF 40 Recommendations

2.5.50 The 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, 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 lower ML/TF risk than customers that are unregulated or subject only to minimal AML/CTF regulation. In determining whether a customer relationship presents a lower ML/TF risk, and therefore whether 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 a risk assessment of 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 1.5.19 to 1.5.27 for more information on SDD.

2.5.51 If the bank establishes that SDD measures 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(s).

Government institutions

EU AML/CTF Directive (EU) 2015/849 Annex II

2.5.52 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 EU AML/CTF Directive. 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, SDD measures may be applied.

Wwft 2(b)2

2.5.53 With respect to customers that 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 ML/ TF risks. Where the bank determines that the customer relationship presents a low ML/ TF risk, SDD measures may be applied. Banks must carry out an appropriate risk assessment on the customer and must establish that there are no indications of higher risks. This assessment must be recorded. Refer to paragraphs 1.5.19 to 1.5.27 for more information on SDD.

2.5.54 When the government institution is organised as a public-law entity (government, municipality, provinces, etcetera) and when the bank establishes that there are no indications of higher ML/ TF risks, banks are not required to identify the UBO(s) for non-totalitarian regimes. For totalitarian regimes there is a risk that those in power abuse their position for their own gain and are in fact the UBO(s). In this case, banks must apply CDD measures in line with EDD measures applicable to PEPs.

2.5.55 In case of a company (e.g. a private limited liability company or another legal entity under private law) that is partially or wholly owned by the government, banks must identify and verify the

UBO(s) in the same manner as for a “regular” company. The exact way of determining the UBO(s) depends on the legal form of the specific private company. Similarly, in case of companies partially or totally owned by totalitarian regimes, there is a risk that those in power abuse their position for their own gain. Consequently, the bank must apply CDD measures in line with EDD measures applicable to PEPs.

Dutch public authorities

2.5.56 Public authorities engaged in public administration are, generally, incorporated by law and often set-up in different forms. Banks should establish that the public authority customer is part of the Dutch government and should verify that the public authority exists. Banks can do so by means of e.g. an extract from the Chamber of Commerce and from official government websites.

A Dutch public authority is 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);
- Bodies of the judicial system;
- Dutch regional water management authorities (in Dutch *waterschappen* or *hoogheemraadschappen*).

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

Dutch semi-public authorities

2.5.58 Dutch semi-public authorities are not fully government owned. Banks need to record the ownership and control structure in the customer file. Examples include public broadcasters, national museums, public libraries, educational institutions, healthcare services and public utility companies.

Supra- or international organisations

2.5.59 International organisations are entities established by formal political agreements between their member states and have the status of international treaties. Their existence is recognised 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 organisations include the UN and affiliated international organisation (e.g. the International Maritime Organisation), regional international organisations (e.g. the Council of Europe, institutions of the EU, the Organisation for Security and Co-operation in Europe and the Organisation of American States), military international organisations (e.g. the North Atlantic Treaty Organisation), and economic organisations (e.g. the World Trade Organisation or the Association of Southeast Asian Nations), etc. Similar to public authorities the CDD on supra- or international organisations must be adjusted to the risks involved.

Religious bodies

2.5.60 A religious body (in Dutch *kerkgenootschap*) is an organisation that aims to make people with the same religion live their faith together. It includes (Christian) churches, and other 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.). Religious organisations can also be established in other legal forms (e.g. a foundation).

2.5.61 Religious bodies can have a higher ML/TF risk because of the large number of (cash) donations they receive, from mostly unknown parties. In addition, the organisation may be used for other activities than just for religious purposes, or may use religion as cover for other activities (e.g. TF, ML and tax fraud). If a religious body has connections with high-risk countries and/ or conflict areas (e.g. missionary work), there exists an extra risk that the religious body is involved in the financing of terrorism in

those countries, as well as an extra risk that the religious body violates sanctions legislation. Finally, since religious body is not a protected concept, and can, in theory, be established by anyone, religious bodies also have a higher integrity risk.

2.5.62 Religious bodies may have an ANBI (in Dutch *Algemeen Nut Beogende Instellingen*) status. This status is granted by the Dutch tax authorities to organisations that meet the applicable conditions. For example, the Dutch 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 organisations. A Dutch religious body may also be affiliated with the Inter-Denominational Contact in Government Affairs.[69]

Even when an organisation has the ANBI status, it can still present an integrity risk. Consequently, banks should always assess the integrity risk of religious bodies, even when they have the ANBI status.

FATF RECOMMENDATION 8

2.5.63 Banks should take into account the FATF and the OFAC guidance on these types of organisations and on the risk associated with religious bodies.

2.5.64 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 on whether it is registered or not.

Implementing Decree Wwft 2018 3(b)

2.5.65 The UBO(s) of a religious body is the private individual who has been appointed as legal successor in the statute of the organisation, upon the dissolution of the organisation. If:

- based on this rule, no UBO can be identified and there are no grounds for suspicion, or
- in cases of doubt, where there is uncertainty whether the individual(s) identified is, in fact, the UBO(s),

.....

[69] Interkerkelijk Contact in Overheidszaken, available at www.cioweb.nl.

the private individual(s) appointed in the statute/ documentation of the organisation as the member(s) of the executive committee in the governing body are identified as UBO(s).

2.5.66 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

Implementing Decree Wwft 2018 3(c)

2.5.67 For the Dutch foundations, associations, mutual benefit associations and cooperatives, the following private individual is defined as the UBO:

1. A private individual who is the beneficial owner of, or has control over the legal entity via:
    - The (in)direct holding of more than 25% of the ownership interest in the legal entitiy;
    - The (in)direct holding of more than 25% of the voting rights regarding amendments to the articles of association of the legal entity;
2. A private individual who otherwise exercises effective control of the customer, based on the responsibility for the strategic decisions that fundamentally affect the daily or regular affairs/ business of the customer. Examples incl. the chairman, the secretary and the treasurer;
3. If the situations described in points 1. or 2. are not applicable, and when there are no grounds for suspicion that there is an UBO as defined in points 1. or 2., all private individuals who hold the position of senior managing official;
4. If there is uncertainty whether the the individual(s) identified is in fact an UBO, all private individuals who hold the position of senior managing official.

2.5.68 Please note that identifying senior managing officials as UBOs can only be done as a last resort, when there are no grounds for suspicions, and in case of doubt. In case senior managing officials qualify as UBOs, the ratio for designating these persons as UBOs should also be stored.

Foundations

2.5.69 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 (e.g. 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 its 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 BV). In the Netherlands, it is mandatory to register the foundation with the Trade Register, but it does not has any legal obligation to deposit financial statements regarding to the foundation.

2.5.70 A foundation has a board, but no members. In general, a foundation has a board existing of different private individuals. When a foundation has only one board member this may pose a potential higher risk of misuse of the foundation because this one private individual has ultimate controle over the foundation. A foundation may operate a business, but its profits must be allocated to the foundation's cause or purpose. The foundation's board members can be paid employees, although this is not usual. Instead, board members usually only receive remuneration for their expenses. Non-profit or charitable organisations are often set up as foundations. They are primarily engaged in raising funds for a specific purpose such as social support, religion, culture, education or other 'good causes'.

STAK

2.5.71 A STAK (in Dutch *Stichting Administratie Kantoor*) is a special type of entity, holding investments and separating the legal ownership – shares or other assets – and the economic ownership. The STAK is the legal owner of the shares/ assests, while the economic interest lies with another entity. The STAK administers the shares for the benefit of the transferor and against the simultaneous issuance of depository receipts (certificates) by the STAK, to the economic owner.

In the case of a STAK (a Dutch type of foundation) as a customer, the following private individual is defined as their UBO:

1. A private individual who is the beneficial owner of, or has control over the STAK via:
    a. The (in)direct holding of more than 25% of the ownership interest in the STAK;

b. The (in)direct holding of more than 25% of the voting rights regarding amendments to the articles of association of the STAK;

2. A private individual who otherwise exercises effective control of the STAK, based on the responsibility for the strategic decisions that fundamentally affect the daily or regular affairs/ business of the STAK;
3. If the situations described in points 1. or 2. are not applicable, and when there are no grounds for suspicion that there is an UBO as defined in points 1. or 2., all private individuals who hold the position of senior managing official; or
4. In cases of doubt, where there is uncertainty whether the private individual(s) identified is, in fact, the UBO, all private individuals who hold the position of senior managing official.

2.5.72 Identifying senior managing officials as UBOs of a STAK can only be done as a last resort, when there are no grounds for suspicions, and in case of doubt. In case the senior managing officials qualify as UBOs, the ratio for designating these persons as UBO should also be recorded.

2.5.73 In case the STAK is not the customer but is on top of the ownership structure of a customer one should look through the STAK to identify the UBO of the underlying company. A certificateholder is a UBO of the underlying company, if the certificates that belong to the holder represent an ownership interest of more than 25%. However one should also consider who has the voting rights. If the STAK has more than 25% of the voting rights on the underlying entity or assets, the directors of the STAK should be considered as UBO of the underlying entity.

FATF Recommendations 8

2.5.74 In assessing the risks presented by NPOs, a bank may distinguish between NPOs that have a limited geographical reach, and those with unlimited geographical reach (e.g. 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 a foreign country, the charity can be expected to transfer funds to that country. Otherwise, it would be unusual for the organisation to transfer funds to a third country, and it would lead the bank to regard the charity as higher risk.

2.5.75 NPOs are suitable vehicles for the financing of terrorists and of terrorist organisations. The risks relate to a possible dubious source of income/ capital and cash donations, unclear (illegal) expenditures, TF, and to the loss of reputation by the bank. Having a CBF quality mark and/ or an ANBI status, does not

guarantee the mitigation of integrity risks. Nevetheless, NPOs that lack a quality mark or registration (e.g. CBF or ANBI) may also be less transparent and lack supervision, thereby only increasing the risks they pose to banks.

2.5.76 In the past, NPOs have been abused for the purpose of diverting funds to TF and other criminal activities. The FATF published a best practices paper on how to combat the abuse of NPOs, in support of its Recommendation 8.[70] In November 2005, the European Commission adopted a Recommendation containing a Framework for a code of conduct for NPOs.[71]

2.5.77 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

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

1. Association with legal personality: the association has the full legal capacity (in Dutch *volledige rechtsbevoegdheid*) and, in theory, there is no personal liability for its obligations. A civil-law notary is needed to draft the deed of the association, stating that the association has been established, and listing its statutes. It is mandatory to register an association with "full legal capacity" at the Ttrade Register. An association with full legal capacity" has the same rights and duties as a private individual (e.g. it can take out loans, own and inherit registered property). Subsidy providers often require that associations have "full legal capacity".
2. Association with limited legal capacity (in Dutch *vereniging met beperkte rechtsbevoegdheid*). They can be established without a notarial deed. The officers of an informal association are held personally liable for its obligations. The liability can be limited by entering the association in the Trade Register. An association with limited legal capacity cannot own registered property (e.g. real estate).

.....

[70] FATF (2015) *Best Practices on Combating the Abuse of Non-Profit Organisations*, available at bit.ly/3spglA3.
[71] EC (2005) *The Prevention of and Fight against Terrorist Financing through enhanced national level coordination and greater transparency of the non-profit sector*, available at bit.ly/3pMrf0P.

2.5.79 An association of owners (Vereniging van Eigenaren (VvE)) is a special type of association. The association is established by operation of the law at the moment a building is devided into apartments (“splitsingsakte”). When an apartment owner buys an apartment, they become automatically a member of the association of owners.

For the association of owners, the following natural persons are identified as UBO:

1. Natural persons who holding (in)directly more than 25% of the voting rights in the association;
2. The statutory directors of the association as listed in the Trade Register based on the fact that they exercise effective control, unless there is an indication that another person exercises effective control.

If the association of owners is professionally managed by an administration office or similar organisation and there is no UBO identified based on voting rights or control, the statutory directors as stated in the trade registration of that organisation are designated as senior managing officials (pseudo-UBO).

In case a legal entity holds more than 25% of the voting rights in the association it must be established whether there is a natural person within that legal entity that qualifies as an UBO of the association of owners (based on voiting rights or based on effective control).

Mutual benefit associations

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

Cooperatives

2.5.81 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” (in Dutch *bedrijfscoöperatie*) and the “entrepreneurs cooperative” (in Dutch *ondernemerscoöperatie*).

- A business cooperative supports the business interests of its members in certain areas (e.g. procurement or advertising). A well-known example in the Netherlands is FrieslandCampina, a large dairy cooperative whose members (dairy farmers) share the cooperative's profits;

- The members of an entrepreneurs' cooperative work independently, but can join forces on certain projects.

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

2.5.82 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" (in Dutch *coöperatie met beperkte aansprakelijkheid*) or a "cooperative with excluded liability" (in Dutch *coöperatie met uitgesloten aansprakelijkheidcooperative*).

Partnerships

2.5.83 A partnership is a community of persons created by an agreement. A partnership is not a legal person (unincorporated), and is therefore not the person with whom the bank establishes a customer relationship or for whom the bank carries out a transaction. There are general partnerships, limited partnerships, similar communities of unincorporated persons, or similar entities governed by foreign law. A general partnership may, for instance, consist of private individuals and/ or legal persons who, together, constitute the company that is the customer of the bank.

Wwft 1(1)

2.5.84 Under the terms of the Wwft, only a private individual or a legal entity can be a 'customer'. Consequently, a partnership cannotnot be a customer. The Wwft assumes that the individual partners (private individuals 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 the individual.

2.5.85 Given the wide range of unincorporated businesses, in terms of size, reputation and numbers of partners/ principals, banks should assess where a particular partnership or business lies on the associated risk spectrum.

2.5.86 When unincorporated businesses are well-known, reputable organisations, with a long history in their industries, and with substantial public information available on them, their principals and controllers, the bank may gather reliable and independent evidence on the customer from the professional or trade

association that the customer is member of. This does not obviate the need to verify the identity of the partnership's UBO(s).

2.5.87 Partnerships may comprise of a small number of partners/ principals. When verifying the identity of these customers, the bank should consider the number of partners/ principals:

- When there are relatively few partners/ principals, the customer should be treated as a collection of private individuals, and banks should follow the guidance set out in section 2.4;
- When there are relatively many partners/ principals, the bank can decide whether to regard the customer as a collection of private individuals, or be satisfied with evidence of the partnership's membership to a relevant professional or trade association.

In both circumstances, the bank should see the partnership, in order to be satisfied that the entity exists, unless the bank can check the partnership's registration in the appropriate national register (e.g. in the Netherlands, VOFs and CVs must be registered in the Trade Register). Banks can also gather additional information from the partnership agreement.

2.5.88 In relation to partnerships (or similar legal arrangements), the following private individual is defined as UBO:

1. Private individual who is the beneficial owner of, or has control over the partnership (or similar legal arrangement) via:
    a. The (in)direct holding of more than 25% of the ownership interest of the partnership (or similar legal arrangement);
2. The (in)direct exercise of more than 25 % of the votes in decision-making with regard to the amendment of the agreement on which the partnership or similar legal arrangement is based, or with regard to the implementation of that agreement other than through acts of management, insofar as in that agreement is prescribed by majority vote; Private individuals who otherwise exercises effective control of the customer based on the responsibility fro the strategic decisions that fundamentally affect the daily or regular affairs/business of the customer;
3. If the situations described in points 1. or 2. are not applicable, and when there are no grounds for suspicion that there is an UBO as defined in points 1. or 2., all private individuals who hold the position of senior managing official; or

4. In cases of doubt, where there is uncertainty whether the private individual(s) identified is, in fact, the UBO, all private individuals who hold the position of senior managing official.

2.5.89 Please note that identifying senior managing officials as UBOs can only be done as a last resort, when there are no grounds for suspicions, and in case of doubt. In case senior managing officials qualify as UBOs, the ratio for designating these persons as UBO should also be stored.

Limited partnership (CV)

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

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, 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 Managing partners are authorised to act on behalf of the 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 is required if the CV runs a business. CVs that do not run a business do not need to be registered in the Trade Register.

2.5.93 Silent partners (also called limited partners), only contribute financially to the CV. They cannot act on behalf of the CV and have no direct influence on the partnership. 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.

Trust and equivalent legal arrangements

2.5.94 A 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 – e.g. the EC published a list of legal arrangements

which qualify as an equivelant legal arrangement of a trust, based on the EU AML/CTF Directive.[72] Trusts are not legal persons according to Dutch law.

2.5.95 Trusts are legal relationships created - inter vivos or on death - by a person, the settlor, when assets are being placed under the control of a trustee for the benefit of a beneficiary or for a specified purpose. In some cases, the settlor appoints a protector or a controller who can remove the trustee, in case of misconduct, and 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;
- The 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 they are accountable, to manage, employ or dispose of the assets, in accordance with the terms of the trust, and with the duties imposed on them by law.

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

2.5.97 There is a wide variety of trusts and legal arrangements (e.g. *anstalt, fiducie, treuhand, fideicomiso*). It is important, when banks evaluate the risks and decide the on the proportionate AML/CTF measures, that they consider the ML/TF risks related to the size, areas of activity and the business of the trust.

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 should be verified as UBOs.

.....

[72] EC (2019) *List of trusts and similar legal arrangements governed under the law of the Member States as notified to the Commission*, available at bit.ly/2NQKZDt.

2.5.99 For trusts (or similar legal arrangements), the UBO(s) include the following:

- The settlor(s);
- The trustee(s);
- The protector(s), if any;
- The beneficiary(ies) or, in case the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of private individuals in whose main interest the legal arrangement or trust is set up, or operates; and
- Any other private individual exercising ultimate control over the trust (or similar legal arrangements), by means of (in)direct ownership, or by other means.

Wwft 4(5)

2.5.100 In some trusts (or similar legal arrangements), instead of being a private individual, the UBO may be a class of private individuals who benefits from the trust. Where only a class of private individuals is required to be identified, it is sufficient for the bank to ascertain and name the scope of the class. It is not necessary for the bank 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 each UBO.

2.5.101 Other “simulair legal arrangements” should be understood to encompass any entity (that is not a private individual), that can establish a permanent customer relationship with the bank or otherwise own property. Examples incl. *anstalt*, *fiducie*, *fonds voor gemene rekening*, *treuhand*, *fideicomiso*.

2.5.102 Where private individuals other than the trustees, the settlor and beneficiaries exercise control over the trust property (e.g. trust protectors), the bank should consider them as UBO(s).

2.5.103 For most trusts, the bank can identify the UBO(s) by reviewing the trust’s constitutions. The UBO(s) is either the identified beneficiary, or a class of beneficiaries.

Wwft 33

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

- The name of the settlor;
- The full name of the trust;
- The nature, purpose and objects of the trust (e.g., discretionary, testamentary, bare);

- The country of establishment;
- The cnames of all trustees;
- The names of any beneficiaries (or, when relevant and as set out in paragraph 2.5.101, a description of the class of beneficiaries);
- The name of any protector or controller; and
- The law governing the trust or other legal arrangement.

2.5.105 Banks must verify the identity of the trust based on documents, data or information obtained from a reliable source, that is independent from the customer. This may require banks to look into relevant extracts from the trust deed (i.e. the agreement on which the trust is based, and by which the trust is managed), or to refer 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 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 (e.g. 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 is sufficient. However, less transparent and more complex structures, with numerous layers, may pose a higher ML/TF risk. Trusts established in countries with favourable tax regimes may be associated with tax evasion and ML/TF risks and banks may therefore require additional information on the purpose, funding and on the beneficiaries of these trust.

2.5.109 Banks should assess whether the trust (or similar legal arrangements) carries a higher ML/ TF risk. Useful information to this end includes:

- Information on the donor/ settlor/ grantor of the funds (except where there are large numbers of small donors);
- The location of business/activity (operating address);
- The nature of business/ activity.

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 TCSPs in the Netherlands is based on the Wtt, the Wwft and the SW. TCSPs can only provide trust services in the Netherlands if they are licenced and supervised by the DNB.

Wtt 1(a)

2.5.111 A TCSP is any private individuals 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, director or secretary for a company, partner for 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 country to country. 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 is a foreign legal form. There are many different legal forms outside of the Netherlands, and they vary per country. In order to determine the UBO(s) and other parties involved with

the customer, the bank must 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 (e.g. whether its capital is divided in shares, whether it has capital, whther the are partners, whether one or more partners may be silent etc.)

Wwft 11(2)(3)

2.5.114 If the customer is a foreign legal entity that is not established in the Netherlands, the bank should verify its identity based on:

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

2.5.115 For foreign legal forms, banks should pay extra attention to:

- The reason the entity wishes 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 (e.g. a legal form that allows anonymous shareholders);
- The extent to which the entity is established in a country other than the country under whose law it is incorporated, as well as the reasons for using a foreign legal form (e.g. entity is a branch);
- The country-specific method of identification and verification of the customer and of parties involved with the customer that deviates from Dutch laws and regulations on identification and verification (e.g. a method of identification and/ or verification that is less strict than in the Netherlands).

Entities that are legally insolvent and/or bankrupt

Identification and verification requirements

2.5.116 The CDD requirements for companies that are insolvent but not in liquidation are the same as for companies that are not insolvent. This is because the company may not necessarily be liquidated and may continue to exist as a legal entity. The bank must however also identify and verify the curator of the insolvent company as UBO, due to control they have.

2.5.117 Companies that are in liquidation may present difficulties in obtaining full information and documentation. The full time driven review should be conducted on a best effort basis.

2.5.118 In all cases, banks are required to:

- Identify and verify any third parties that hold effective control over the company. Parties that hold effective control qualify as UBO(s). A curator, liquidator, or receiver, may fulfill this role depending on the extent to which they control the company;
- Identify and verify any party that has legal authority to represent the company. Parties that have the legal authority to represent the company should be considered as authorised representatives. In almost all cases the curator, the liquidator, or the receiver fulfils this role;
- Obtain proof of their control;
- Conduct background screening on the controller and of any other relevant third party;
- Ascertain the rationale for the third party contributing to the company estate;
- Ascertain the source of funds of the third party, if they are providing a deposit or other financial assistance.

CDD risks specific to companies that are insolvent and/or in liquidation

2.5.119 The risk profile of a company that is insolvent and/or in liquidation can change depending on how the status of the company is affected by the proceedings. There is a number of know schemes related to bankruptcy liquidation. Examples incl.:

- Concealment: Removing everyting of value from a company before bankruptcy is declared. The assets can therefore not be resold by the liquidator.
- Collusion: Repaying certain creditors (often associated with the debtor via complex ownership structure) first so there is no money remaining for the rightful creditors.
- Bustout: A company is set up with the intention to ultimately file for bankruptcy. Goods are then obtained and sold for cash, without paying suppliers. Bankruptcy is then declared.

To identify such a fraudulous scheme or to the identify the risks hereof, banks can:

- Conduct a transaction check for any (potentially) suspicious transactions; and
- Establish the plausibility of the source of funds, if there are any flows from third parties – e.g. loans from third-parties.

2.6 Multipartite relationships, incl. reliance on third parties (introduction and outsourcing)

2.6.1 Often, a customer may have contact with two or more institutions (see 2.6.3) in respect of the same transaction. This can be the case in 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 (e.g.syndicated lending, where several institutions may participate in a single loan to a customer).

2.6.2 While several institutions requesting the same information from the same customer in respect of the same transaction helps prevent ML/ TF, it also inconveniences the customer. Each institution must, therefore, be clear as to its relationship with the customer, to the extent to which it has complied with its AML/ CTF obligations, and to the extent to which it relies on (or otherwise takes account of) the verification of the customer carried out by other institutions. Banks should take account of the identification and verification conducted by other institutions on a risk-based manner.ML/ TF. Banks should also consider that some of the institutions involved may not be EU-based and may therefore not meet the requirements as laided down in the EU AML/ CTF Directive

2.6.3 Institution A may rely on Institution B to carry out CDD measures, while remaining ultimately liable for compliance with the Wwft, when, e.g.:

- Institution A enters into a customer relationship with, or undertakes an occasional transaction for, the underlying customer of Institution B - e.g. 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).

Paragraph 2.6.6 details what kind of institution Institution B must be to allow this reliance.

2.6.4 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 2.6.13 – 2.6.14.

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

2.6.5 Banks may rely on a third party carrying out aspects of CDD. This is possible in the following situations:

- "Introductory CDD" by another institution subject to Wwft regulation, which has already completed aspects of CDD; or
- "Outsourcing CDD" as part of an outsourcing agreement or agency agreement.

Introductory CDD

2.6.6 A bank may rely on the CDD performed by another institution as long as the latter is subject to the Wwft. The following Wwft-institutions may carry out CDD as an introducing party:

- Tax advisors with a registered office in an EU/ EEA Member State;
- Accountants with a registered office in an EU/ EEA Member State;
- Lawyers with a registered office in an EU/ EEA Member State;
- Notaries with a registered office in an EU/ EEA Member State;
- A profession/ business similar to that of a lawyer or of a notary, with a registered office in an EU/ EEA Member State;
- Trust and Corporate Service Providers, licenced under the WTT 2018;
- Banks and branches of banks with a registered office of place of business in an EU/ EEA Member State;
- Other financial companies and branches of financial companies with a registered office of place of business in an EU/ EEA Member State;
- Branches (or majority owened subsidiaries) of banks and other financial companies with a registered office in an EU/ EAA Member state, which are registered in a non-EU Member State, in case the branch (or majority owned subsdiary) is part of the same Group and fully complies to the Group policies and procedures.

Buyers and sellers of goods (i.e. traders), intermediaries, gambling supplier and valuers cannot act as introducting party.

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

2.6.7 The following must be taken into account when making use of Introductory CDD:

- The bank is and remains at all times responsible for identification and verification;
- It may not lead to any deterioration in the quality of the bank's own independent assessment;
- The bank must have sufficient insight and assurance that the procedures, measures and expertise of the introducing party meet the required standard;
- The bank has a clear policy and procedures in case of structural use of Introductory CDD. Part of the bank's AML/ CTF policy statement must 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) (see paragraph 2.6.7);
- A bank must document the steps taken to confirm that the institution relied upon satisfies the requirements in Wwft article 5 (1)(a). This is particularly important when the institution relied upon is registered outside the EEA. It is prohibited to place reliance on third parties established in high-risk countries as designated by the EU Commission.

2.6.8 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 the CDD themselves.

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

- The public disciplinary record of the third party, to the extent that this information is available;
- The nature of the customer, the product/ service sought and the sums involved;
- Any adverse experience regarding the general efficiency in business dealings of the third party;
- Any other knowledge, whether obtained at the outset of the relationship or subsequently, that the bank has regarding the standing of the third party;
- Knowledge that relevant CDD requirements were carried out, by the third party, in accordance with the Wwft (or with equivalent legislation in international situations).

Wwft 5(1)(c)

2.6.10 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 UBO and/or the authorised representative.

Outsourcing CDD

Wwft 10

2.6.11 According to article 10 Wwft a bank may outsource CDD measures to an agent or to an outsourcing service provider, as long as the arrangements between the bank and the agent or the outsourcing service provider stipulate that the bank remains liable for any failure to apply such measures. Furthermore, it is not allowed to outsource the ongoing monitoring obligation on the customer relationship, unless the outsourced party belongs to the same banking Group.

2.6.12 The bank must document outsourcing arrangements when they are of a structural nature. The bank may consider drawing-up standard 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 (incl. arrangements on making information available at the request of supervisory authorities);
- That supervisory authoritieshave 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.

Group introductions

Wwft 5 (1)(a)(5°), (2)

2.6.13 Where customers are introduced between different parts of the same 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 the Wwft, the EU AML/ CTF Directive, or with an equivalent AML/ CTF standard. One member of the Group should be able to

demonstrate to another member of the Group that the identity of the customer has been appropriately verified.

2.6.14 Where a customer is introduced by one part of a Group to another, it is not necessary the latter to re-verify the customer's identity, 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 EU AML/ CTF Directive or with an equivalent AML/ CTF standard;
- 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 (or 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 EC) where those branches (or majority-owned subsidiaries) fully comply with the Group-wide AML/ CTF program.

Situations which are not considered to be reliance

(i) One institution acting solely as introducer

2.6.15 An institution may act solely as an introducer of the customer to the bank and may have no further relationship with the customer. In this case, the introducing institution 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. An example hereof is the name-passing broker in inter-professional markets.

2.6.16 When the introducing institution 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 preclude the introducing institution from carrying out identification and verification of the customer on behalf of the bank, as agent for that bank (see paragraphs 2.6.19 and 2.6.20).

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

2.6.17 If the intermediary is an agent or appointed representative of the product or service providing bank, the intermediary is an extension of the bank. The intermediary may obtain the appropriate verification evidence in respect of the customer. In this case, the product/ service providing bank is responsible for specifying what the intermediary must obtain, and for ensuring that the records of the appropriate verification of the evidence are correctly retained.

2.6.18 Similarly, where the product/ service providing bank has a direct sales force, the sales force is part of the bank, irrespective of whether they operate under a separate Group. The bank is responsible for specifying what is required, and for ensuring that records of the evidence verification evidence taken are correctly retained.

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

2.6.19 From the point of view of a product/ service providing bank, 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 EU AML/ CTF Directive or to similar legislation in a low-risk country. The intermediary may be regulated, may be based in the Netherlands, elsewhere within the EU, or in a country outside the EU, which may or may not be a member of the FATF. Guidance on assessing which countries might be low-risk countries is given in Annex 1-I.

2.6.20 If the intermediary carries on appropriately regulated business and is acting on behalf of another party, the bank may decide to carry out CDD measures appropriate for lower risk situations on both the intermediary and on the underlying customer, if the bank assesses that the country where the intermediary is registered, the situation, the product it provides and the underlying customer, all carry low ML/ TF risks.

2.6.21 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.

2.6.22 Where the bank takes instruction from the underlying customer, or where the bank acts on the underlying customer’s behalf (e.g., as custodian) the bank has an obligation to carry out CDD

measures in respect of that customer, although the reliance provisions may be applied.

2.6.23 In these circumstances, in verifying the identity of the underlying customer, the bank may take a risk-based approach. The bank needs to assess the AML/ CTF regime in the intermediary's country, 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 directly from the customer.

2.6.24 In particular, where the intermediary is located in a higher-risk country, 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 customer has been verified to the satisfaction of the product/ service providing bank.

2.7 Monitoring customer activity

The requirement to monitor customers' activities

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

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

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

2.7.2 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

2.7.3 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 ML/ TF riskML/ 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 & Section 5 DNB Guidance on the AML/ CTF Act and Sanctions Act

2.7.4 In determining the risk profile of the customer and/ or customer peer groups, banks also include the expected transaction behavior of the customer or of the peer group to which the customer belongs. Banks can categorize their customer into peer groups. Peer groups can be formed on the basis of a number of customer characteristics – e.g. customer segment, sectors, country of incorporation, legal form, countries in which the customer is active, etc. By using peer groups to create transaction profiles for its customers, a bank can monitor transactions conducted throughout the duration of the customer relationship, and ensure that they are consistent with the knowledge the bank has on the customer and with the customer risk profile.
Depending on the risk, mass retail customers could be included in homogeneous peer groups. To effectively monitor customer behavior, actual transaction behavior is compared to the customers risk profile or to the transactional behavior of a customers' peer group. A customer stays within their 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

2.7.5 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)

2.7.6 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 on effectiveness.

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

2.7.7 Banks must have adequate reporting and alert handling processes. Banks must further ensure that intended and executed unusual and suspicious transactions[73] are reported to the FIU, without delay, and in line with the reporting requirements. Banks should use a case management system so that all actions are recorded and so that 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 supervisory authorities identify a 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

2.7.8 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)

2.7.9 Monitoring customer activity is aimed at identifying suspicious activity. In order to understand what is unusual, banks first need to identify the customer transaction profile. A transaction profile of a customer is based on the bank’s expectations on the customer transactions or on the cusomer’s use of their account. A bank can also make use of peer groups to establish a transaction profile.

By creating a transaction profile, banks can monitor whether the transactions carried out during the term of the customer relationship correspond with the knowledge the bank has of the customer and the customer’s risk profile.

In case a transaction profile per customer is created, this transaction profile is:

- Current: the transaction profile is up-to-date and has a date. All relevant changes to the profile are made promptly;

.....

[73] 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’.

- Complete: it includes all bank account numbers, names of beneficiaries, and the people authorized to make payments and all relevant activities
- Specific, substantiated and clear: the expected flows are clearly described in terms of e.g. amounts, services and frequency. The (tresholds) amounts indicated are well-substantiated and can actually contribute to recognizing unusal transactions
- Must be 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 customer relationship allows banks to know their customers and to assess risks, and provides greater assurance that the bank is not being misused 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

2.7.10 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 file external reports. Executed or proposed SARs must be notified to FIU, without delay, upon the identification of their unusual nature.

Transactions are deemed unusual if they meet the objective or subjective indicators mentioned in the Appendix of the Implementing Order of the Wwft.[74] 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, their behavior or the context are not decisive in this situation. Only the hard facts of the transaction are decisive. In addition:

.....
[74] Appendix of the Implementing Order of the Wwft, available at bit.ly/31de7rD.

- 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 (these transactions are already assumed to be related to ML/ TF);
- Transactions involving an objective indicator are called 'evidently SARs' and must therefore be reported to FIU, without delay.

Subjective indicator
A subjective indicator is a transaction where the institution has reason to assume the transaction can relate to ML/ TF. In this situation:

- Not only the individual transaction is decisive, but also transaction patterns and (the behavior of) the customer;
- No limit is set for the subjective indicator;
- Important is the opinion of the staff regarding the unusual nature of the transaction.

Section 5 DNB Guidance on the AML/ CTF Act and Sanctions Act

2.7.11 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

In either case, SARs or activities must be flagged for further examination.

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

2.7.12 Monitoring may be done by referencing to specific types of transactions, to the profile of the customer, or by comparing their activity or profile with that of similar customers (i.e. peer group), or through a combination of these approaches.

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

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

2.7.14 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.

2.7.15 Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. The scope and complexity of the process depends on the business activities, and on the size of the bank. The key requirements of any well-functioning monitoring system are:

- Having up-to-date customer information, on the basis of which it will be possible to spot the SARs/ activities; and
- Asking pertinent questions to elicit the reasons for the SAR/ activity, in order to judge whether they may represent anything suspicious.

Nature of monitoring

Wwft 8

2.7.16 Higher-risk accounts and customer relationships require enhanced ongoing monitoring – i.e. more frequent or intensive monitoring.

Manual or automated?

2.7.17 A monitoring system may be manual, or may be automated (to the extent that the automated system produces a standard suite of exception reports – i.e. alerts). Banks may chose either one of these approaches. Where issues of volume, or where factors make a basic exception report regime inappropriate, banks may chose for a more sophisticated automated monitoring system.

2.7.18 Banks must recognize the essential importance of staff alertness. 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

2.7.19 In relation to a bank's monitoring needs, an automated system may add value in addition 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, and must be able, if requested, to explain them to a regulator.

2.7.20 There are many automated transaction monitoring systems available on the market. They use a variety of techniques to

detect and report unusual/ uncharacteristic activity. Transaction monitoring 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 due to their heavy reliance on customer reference data and transactional data.

2.7.21 Monitoring systems, manual or automated, can vary considerably in their approach to detecting and reporting unusual or uncharacteristic behavior. Banks must rely on internal assessments (e.g. what is required by their particular business) and on questions asked to the suppliers of monitoring systems (e.g. what can different suppliers deliver) when chosing which solution can best support their business needs. Banks must address questions – e.g.:

- How does the solution enable the bank to implement a risk-based approach to monitor its 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?

2.7.22 What constitutes unusual or uncharacteristic behavior by a customer, is often defined by the monitoring system. It is important that the selected monitoring system has an appropriate definition of 'unusual' or 'uncharacteristic', that is in line with the nature of business conducted by the bank.

2.7.23 The effectiveness of a monitoring system (automated or manual) in identifying unusual activity depends on the quality of the

parameters that determine its alerts, and the ability of staff to assess and act on the alerts. Each bank has specific needs, and each monitoring system varies in its capabilities according to the scale, nature and complexity of the business. Banks must strik the right balance in setting the level at which an alert is generated – i.e. it is not enough to set the monitoring system such that it generates just enough output for the existing staff to deal with; but equally, the monitoring system must not generate many 'false positives' which exhaust the investigation resources.

Alert handling

Wwft 16

2.7.24 Based on the expected transaction profile of a customer, banks must check and conclude on:

- Whether the actual transactions are consistent with that profile;
- Whether the amounts involved match the expected transaction behavior;
- Whether the frequency of the transactions reflects the expected transaction behavior;
- Whether the time frame for the transactions is in line with the expected transaction behavior;
- Whether the total volume of the transactions reflects expected transaction behavior;
- Whether a reasonable suspicion that the transaction(s) may be related to ML/ TF exists;
- Whether a reasonable suspicion that the transaction(s) may be related to other types of crime (e.g. tax evasion) exists; and
- Whether the alert should be escalated and subsequently reported as an SAR.

CDD reviews

Wwft 3 (5), Directive (EU) 2015/849 2018/843

2.7.25 Continuous monitoring of the customer relationship and of the transactions carried out during the course of the customer relationship must be performed, in order to ensure that these correspond to the bank's knowledge of the customer and to the customer risk profile, and must include, when necessary, an examination of the source of the resources used in the customer relationship or in the transaction.

2.7.26 Banks may carry out a review of the customers' due diligence files at different fixed moments within the customer life cycle (also

known as time driven review) and/ or when driven by an event (also known as event driven review). In the absence of an event driven review, banks must have a time driven review in place to ensure that the customer file is continuously reviewed (see paragraph 2.7.40).

Section 3.4 DNB Guidance on the AML/ CTF Act and Sanctions Act

2.7.27 The bank compiles and assignes a risk profile to the customer, based on the performed CDD. This risk profile is dynamic and can change over time. A review serves to determine whether the customer still meets their assigned risk profile. To that end, the bank msut periodically update all customer data (incl. the customer's risk profile, contact information and UBO(s) information). The frequency and depth of the review depends on the risks presented by the customer.

The scope and definition of CDD reviews

2.7.29 CDD review can be triggered by events[75] or by time. Expiry of time is the moment that triggers a review if no event has occurred in the meantime. 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 an event triggered CDD review needs to be performed.

2.7.30 Events can be categorised into:

(1) Bank-driven events (change in (interpretation of) regulatory requirements, policy, market developments, etc.) – e.g. 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.

2.7.31 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, the bank needs to determine how soon the review of the impacted customers/ customer groups must be finalised;

.....

[75] An event is defined as a change in the customer data or in the 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.

- For customer-driven events, the bank needs to assess themas 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 time driven review, this could lead to an extension in the scheduled time driven review.

Section 3.4 DNB Guidance on the AML/ CTF Act and Sanctions Act

2.7.32 The bank is responsible for keeping its customer files up-to-date. In case a bank only uses the event driven review of the customer files (to keep the customer files up-to-date), the scenarios that could initiate an event driven review are demonstratably sufficiently effective.

Starting point of CDD reviews / guiding principle of CDD reviews

Event Assessment

2.7.33 The starting point is to assess whether the trigger constitutes an event that has not yet been identified. If the event has already been identified 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

2.7.34 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 time driven review date.

Execution of the CDD Review

2.7.35 The outcome of the assessments mentioned in paragraphs 2.7.33 and 2.7.34 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 – e.g. a change in director(s), a customer name change, a 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 performing screening, where applicable. The date of the time driven CDD review remains unchanged.

(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 date of the time driven CDD review remains unchanged.

(3) Event Driven Review - The change is material and a full review of the customer needs to take place. Completion of the CDD review changes the date for a time driven CDD review, in line with the customer's risk classification.

Event Driven Review Triggers

Section 4.2.5 DNB Guidance on the AML/ CTF Act and Sanctions Act

2.7.36 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 (e.g. in good standing, insolvent, in liquidation, bankrupt, etc.);
- Change in country risk (e.g. country of domicile, of operation or of activity);
- Change in ownership, tax, and/or shareholder structure;
- Change in UBO(s);
- Change of person(s) acting as authorised representative(s) of the customer (e.g. officers, directors, authorised representatives);
- Material change in business activities, type of business, or 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 patterns (incl. 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 regulations and listings;
- There are indications that the customer may be involved in sanctions violations;
- 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 (incl. SAR filings);
- There are indications that the customer may be involved in ML or TF;
- There are indications that the customer may be involved in other criminal activities;
- Relevant warrant received / customers assets frozen by order of competent authority.

Scope and definition Periodic Reviews

Section 4.3.2 DNB Guidance on the AML/ CTF Act and Sanctions Act

2.7.37 The ML/ TF risk of a customer can change. Banks must therefore carry out periodic reviews to ensure 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 catecory of customer - e.g. 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, the bank must check whether all relevant information and/ or documentation still reflects the actual situation of the customer.

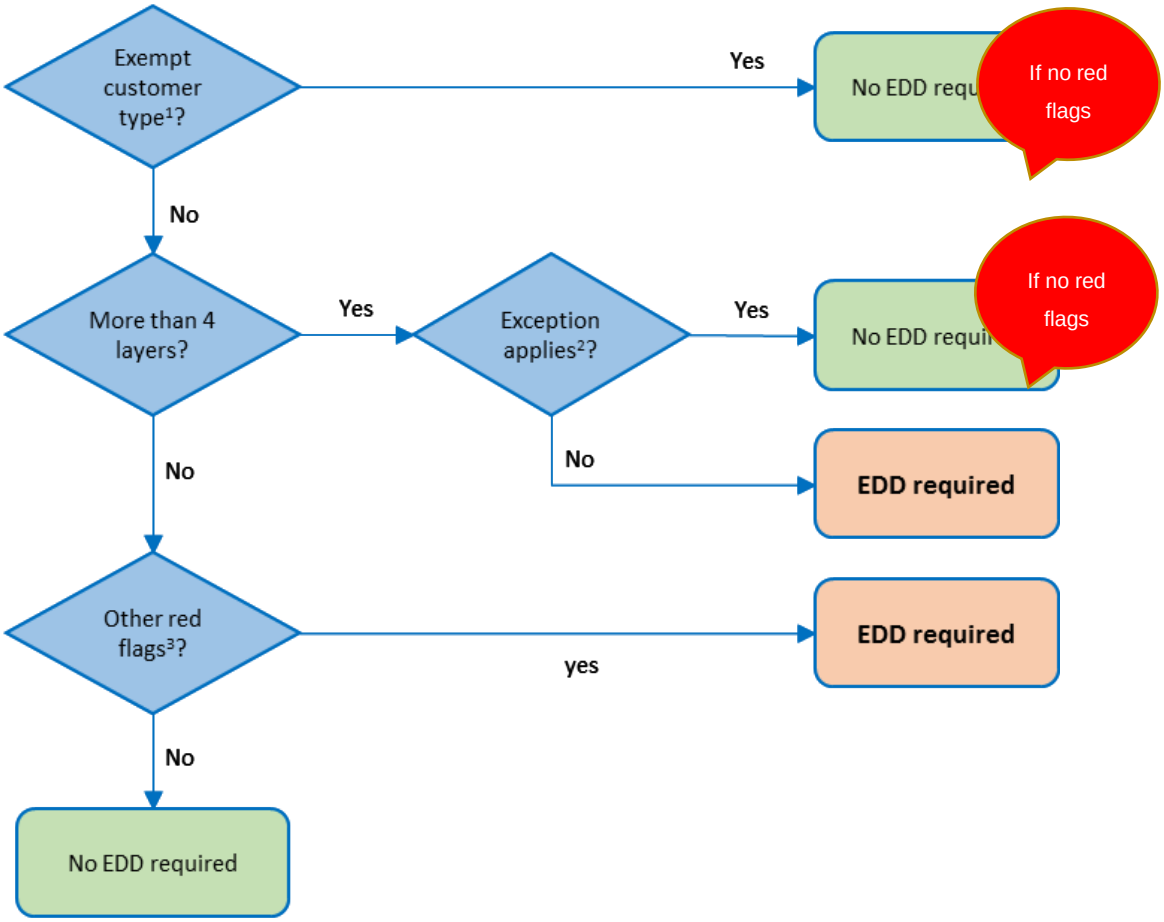
2.7.38 However, in case of mass retail customers, a periodic review might not be required, if sufficient controls are in place to identify, assess and, where necessary, act upon any changes in the customer's risk profile (incl. the identification of any suspicious transactions). In these situations, even when no changes have occurred since the previous review, 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.

2.7.39 After completion of the CDD for new customers, the minimum frequency of the periodic review is then determined (i.e. the next scheduled review date). The CDD file includes the date that the last review was performed, as well as the information obtained

during the review and the renewed risk assessment. Periodic 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 Ownership and control structures

EDD measures on complex structures: decision tree



[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 UBO(s) to establish control disproportionately to the amount of ownership they have in each 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 – i.e. ordinary shares or common shares. Increasingly however, even very small private companies start having different share classes. This may be done to – e.g. be able to vary the dividends paid to different shareholders, or 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 whichever name it chooses. Apart from ordinary shares, common types are preference shares, non-voting shares, A shares/ B shares, etc. (also known as alphabet shares), shares with extra voting rights (also known as management shares). 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 (e.g. 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 to govern how the company is run.

A shareholders' agreement:

- Lasy down the shareholders' rights and obligations;
- Stipulates which shareholders can appoint which executive and non-executive directors;
- Regulates the sale of shares in the company;
- Describse how the company is going to be run;
- Provides an element of protection for minority shareholders and the company; or
- Defines how important decisions are to be made.

4. VIE structure

Another example of a contractual arrangement between shareholders is the Variable Interest Entity (hereinafter VIE) structure. A VIE is 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 (usually an exempt limited company in the Cayman Islands), a China wholly foreign-owned enterprise (hereinafter 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 licenced 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-owned business is a commercial organisation in which ownership and/ or control is in the hands of a family – related by blood, 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 of future generations;
- To allow the easy transfer of ownership or of profit rights to the 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.

Shares can also be held by minors. In such case the voting rights are typically be exercised by a parent. Both may be considered UBOs.

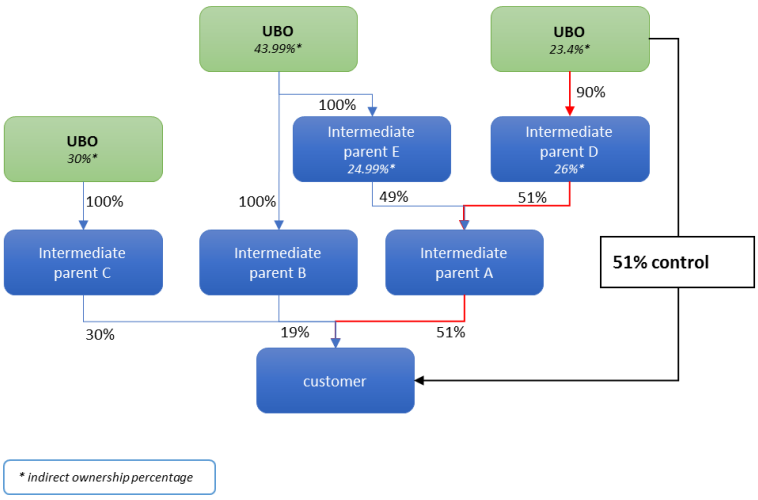
6. Usufruct
Usufruct (in Dutch *vruchtgebruik*) is a legal right in many civil law countries accorded to a person or to a party, that confers the temporary right to use and derive income or benefit from someone else's property (e.g. shares). The owner (the “bare owner”) passes the voting and profit rights of their 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.

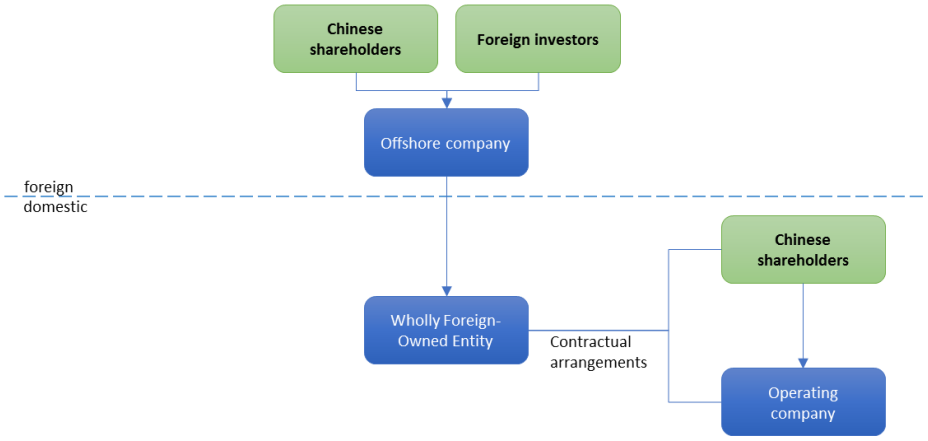
8. Parallel UBO structures
A customer can have multiple branches of ownership leading up to the same UBOs, while all direct and intermediate shareholdings stay below the thresholds of more than 25% that are generally stipulated by international AML/ CTF legislation. For this reason it is important to 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



Chapter 3

Suspicious activities, reporting and data protection

3.1 Evaluation and determination by the relevant officer / identified staff

EU 2015/849 8 (4a) and 33 (2), Wwft 2d (2)(3) and 16

3.1.1 Which staff member has to file a report in case of an unusual transaction or a suspicion of ML/ TF can vary per country. In the Netherlands, the SAR filing to the FIU is the responsibility of the Compliance officer. Throughout this Guidance, the staff member who has this responsibility is deemed the “relevant officer”.

3.1.2. The relevant officer must determine whether a report gives rise to knowledge or suspicion, or to reasonable grounds for knowledge or suspicion. The bank must permit the relevant officer to have access to any information, including ‘know your customer’ information in the bank’s possession, which could be relevant. The relevant 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 their own record-keeping requirements). Any approach to the customer or to the intermediary should be made sensitively, and (probably) by somebody else than the relevant officer, to minimize the risk of alerting the customer or an intermediary that a reporting to the FIU is be being considered.

3.1.3 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 the bank must assess whether a transaction can or must be regarded as an SAR.

3.1.4 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 relevant 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.

3.1.5 If the relevant 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

Reporting to the FIU

Wwft 16 (1) and (4)

3.2.1 The bank's relevant officer must file a SAR to the FIU in the following circumstances:

- Any (intended) transaction or activity that, after evaluation, the bank knows or suspects, or for which the bank has reasonable grounds to know or suspect ML/ TF; (*subjective indicators*)
- Any (intended) transaction based on thresholds included in the Wwft and lower regulations (*objective indicators*);
- Situations where the bank could not successfully conclude its CDD process and there are indications that the customer is involved in ML/ TF;
- Where the bank decides that the customer is unacceptable and ends the relationship, and there are indications that the customer is involved in ML/ TF;
- where the bank when freezing funds on the basis of a 'hit' on the sanctions lists and identify SARs based on an assessment of the transaction history.

3.2.2 Banks must also report SARs that have taken place prior to the establishment of a customer relationship, but which have come to their attention during the provision of their services. Moreover, a direct or causal connection between the unusal transaction and the services provided is not required; the reporting obligation is also trigged where the bank is aware of the transaction (passive involvement).

3.2.3 Banks must report any SAR to FIU, as soon as possible (in Dutch *onverwijld*), after they have become aware of the unusual nature of the transaction.

3.2.4 Reports can be made via the FIU's digital reporting portal, which is available through the FIU's website. It is required to register as an obliged entity in advance.

Wwft 16 (2)

3.2.5 Banks must include in their reports to the FIU all relevant information about the customer, transaction or activity that it has in its records. The statutory minimum of information is:

- The identity of the customer;
- The identity of the UBOs;
- The nature and number of the identity document of the customer;
- The nature, time and place of the transaction(s);
- The size, destination and/or origin of the money, securities, precious metals or other values involved in the transactions;
- The circumstances based on which the transaction is considered unusual.

To the extent possible, the following must also be stated:

- The identity of the person on whose behalf the transaction is carried out;
- The nature and number of the identity document of the person for whom the transaction is carried out;
- The nature and number of the identity document of the UBO(s).

3.2.6 Banks must file SARs to the FIU that are as complete as possible. Specifically, in the case of SARs based on subjective factors, based on a CDD that can not be completed, or on an ended customer relationship, it is important that banks provide a description of the situation and demonstrate how the circumstances contribute to the unusual character of the transaction.

3.2.7 Banks must keep record of their SARs in way that allows them to reconstruct the underlying transactions. The records must include a copy of the submitted SAR, the information submitted with the SAR, and the acknowledgement of receipt from the FIU. The information must be kept for five years from the moment the SAR was submitted, or (in the case of acknowledgement of receipt) from the date the FIU acknowledges its receipt.

3.2.8 Banks must record their SARs and additional information in such way that it allows supervisory authorities to reconstruct and review the banks' assessment, and to determine if the banks have complied fully on a timely basis with their reporting obligation.

Wwft 17

3.2.9 The FIU has the right to request further information to reporting entities, in addition to the intelligence they already presented. Banks must fully cooperate with these requests, by promptly providing the FIU, with all required information. Banks often provide this information in writing, but, in emergency situations, they cab provide them also orally. The FIU has the right to request information data or information from an institution that has filed a SAR, and also other institutions if, in the opinion of FIU, the latter have data or information relevant to the FIU's analysis of an (anticipated) transaction or customer relationship. Banks should, as matter of best practice, have a single point of contact that controls all contact beween departments/ branches and law enforcement agencies, in order to maintain an informed overview of the situation.

3.2.10 Banks should be able to respond promptly to information requests from the FIU or from the supervisory authorities, on whether they maintained a customer relationship with a certain customer and on the nature of that relationship. To this end, banks should have systems in place that allow them to respond promptly and accurately to these information requests. The systems should be adequately secured to guarantee the confidentiality of the information requests and of the information provided to these authorities. The intelligence value of a SAR is related to the information quality of the SAR. Banks must have good databases from which to draw the information to be included in the SAR. Moreover, banks must have a system that allows them to produce (in hard copy) the information requested under a court order by law enforcement agencies.

Wwft 23a

Banks should share SAR information with the other entities of their Group (i.e. with other entities, or with their branches, or majority owned subsidiaries established in third countries), provided that the latter fully comply with the Group-wide policies and procedures (incl. procedures for sharing information within the Group), and to the extent allowed by confidentiality rules and by applicable local privacy laws.

Indemnification

Wwft 16, 17, 19, 20, 20b

3.2.11 Banks that file SARs and that respond in good faith to information requests from the FIU, are protected under article 19 of the Wwft (which provides the ground for criminal

indemnification) and under article 20 of the Wwft (which provides the ground for civil indemnification). Criminal indemnification ensures in such way that such data or information provided by a bank that reports an SAR in good faith cannot be used in a criminal investigation or prosecution of that bank on suspicion of ML/ TF. The Wwft extends this indemnification to those bank staff who submitted the SAR report or helped compiling it. Banks should also ensure that their directors, officers and staff, who report suspicions of ML/ TF internally or to the FIU, are protected from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions.

3.2.12 It is possible that a third party holds a bank accountable in civil proceedings. The Wwft provides civil indemnification. This means that a bank cannot be held liable under civil law for the loss suffered by another party (a customer or a third party) as a result of the bank filing an SAR or responding to an information request from the FIU, as long as the bank acted on the reasonable assumption that it was exercising its reporting duty. For instance, claims in civil proceedings could be brought against the bank, for breach of contract, if the bank decided not to carry out a transaction but to report it in a SAR.

3.2.13 The indemnification only applies if the bank submitted the SAR correctly, in good faith, and in accordance with the Wwft requirements.

3.2.14 A bank may not impair its staff, who filed, on the bank's behalf, a SAR or who responded, in good faith, to information requests from the FIU. This protection extends also to staff who make internal reports of Wwft violations. If such violation occurrs, the staff have the right to file a complaint with the relevant supervisory authority.

Confidentiality when filing SARs and when responding to information requests from the FIU

Wwft 23

3.2.15 The Wwft imposes a strict duty of confidentiality. Banks are obliged to enforce confidentiality with respect to a SAR and to (responses to) information requests from the FIU. Banks may also not tip off their customers and/ or third parties.

Exceptions to the strict confidentiality regime are possible insofar as they have a legal basis. A relevant exception for banks concerns intra-Group sharing of information. Banks are allowed to share information through announcements (in Dutch

mededelingen), including the fact that an unusual transaction report has been filed, with units of its own organisation when these are established in an EU/EEA Member State as well as other units of the organisation that are established in a third country and which comply with the applicable group policies and procedures. Banks are also allowed to share information with other banks in case (i) the information concerns a customer's transaction involving both banks, (ii) the banks are both established in an EU/EEA Member State or equivalent third country and (iii) the information is solely used to prevent ML/ TF. The actual sharing of documents, such as SARs, is not possible under the Wwft. Without these exceptions, existing early-warning systems, such as the interbank warning system, could be obstructed.

3.3 Data Protection - Subject Access Requests, where aSAR was filed

Wwft 22

3.3.1 Occasionally, a Subject Access Request under the General Data Protection Regulation (hereinafter GDPR) will include within its scope one or more SARs, which have been submitted in relation to that customer. Banks should not assume that this kind of information cannot be disclosed in order to avoid tipping off, even though, in practice, it is rarely disclosed. Instead, all Subject Access Request should be carefully considered on their merits, in line with the principles detailed below.

3.3.2 An individual who makes a request in writing (a Subject Access Request) to a data controller (i.e. any organisation that holds their personal data) is normally entitled to:

- Be informed whether the data controller is processing (incl. merely holding) their personal data; and if so
- Be given a description of that data (incl. the purposes for which the data is processed and to whom the data is or may be disclosed); and
- Have communicated to them (in an intelligible form) all the information that constitutes their personal data, and any information available to the data controller as to the source of this data.

GDPR 23, UAVG 41

3.3.3 Article 23 of the GDPR and article 41 of the Implementing Act of the General Data Protection Regulation (in Dutch *Uitvoeringswet Algemene verordening gegevensbescherming*) (hereinafter UAVG) state that personal data are exempt from disclosure in any case where the application of that provision would likely

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 of the UAVG exemption, it is not obliged to inform the individual that any information has been withheld. The information in question can simply be omitted and no reference may be made to it, when responding to the request.

Wwft 22

3.3.5 Each Subject Access Request must be considered on its own merits. Banks must determine whether, in that specific case, the disclosure of a SAR filing is likely to prejudice an investigation and, if consequently, it would constitute a tipping-off offence. In determining whether the article 41 of the UAVG exemption applies, banks may legitimately 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. Banks may also legitimate take account of the confidential nature of SAR filings when considering whether the exemption under article 41 of the UAVG applies.

3.3.6 Whenever disclosure is made in legal proceedings or in a investigation and the full contents of such a disclosure are already revealed, it is less likely that the exemption under article 41 of the UAVG applies. However, banks shoud exercise caution when considering disclosures made in legal proceedings, for the purposes of article 41 of the UAVG exemption, as often disclosures are limited strictly to matters relevant to those proceedings, and other information contained in the original SAR may already be revealed.

Wwft 22

3.3.7 In order to guard against a tipping-off offence, a bank must ensure that no information relating to SARs is released to any person without authorisation. Further consideration may need to be given to SARs received internally that were not submitted to the FIU. Banks should keep a record of the steps they took to determine whether the disclosure of an SAR involves tipping off and/ or whether the article 41 of the UAVG exemption applies.

Wwft 34a(1)(2)

3.3.8 Before entering into a customer relationship or executing an occasional transaction, a bank should inform its customer about

the obligations of the Wwft and about the processing of the customer's personal data in relation to the prevention of ML/ TF.

Any personal data collected on the basis of the Wwft, may only be processed to prevent ML/ TF. This personal data may not be used for any other (e.g. commercial) purposes.

3.4 Whistleblowing

Wwft 20a Wwft

3.4.1 Banks must have procedures that enable staff to file internal reports of any violations committed by the bank. The person reporting the Wwft violations must be able to do so independently and anonymously, and in line with the Whistleblowers Authority Act (in Dutch *Wet Huis voor klokkenluiders*) under which employers must enable their staff to file reports internally.

Chapter 4

Sanctions

SW, Section 7 DNB Guidance on AML/ CTF Act and Sanctions Act

4.1 The SW and the regulations derived from it transpose international sanctions regimes, especially those of the UN and the EU, into Dutch law. The Regulation on Supervision pursuant to the Sanctions Act 1977 (in Dutch *Regeling Toezicht Sanctiewet 1977*) prescribes that an institution must take measures to screen whether its relationships appear on one or more sanctions lists (e.g. the EU decisions and/or regulations, decisions by the Dutch Minister of Foreign Affairs based on the Dutch regulation on terrorism sanctions (in Dutch *Sanctieregeling Terrorisme 2007-II,* also known as the Dutch List) – or UN Security Council Resolutions). The EU 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.

Sanctions hits

Sanctions Act 1977

4.2 Banks must take measures to ensure that they can identify relationships that correspond with private individuals or legal persons and entities that are referred to in the sanctions regulations. Banks must 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 customer 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 a private individual or legal person or entity that is referred to in the sanction's regulations (only genuine hits are reported; 'false positives' are not), the bank must report this immediately to the supervisory 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 (incl. 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 sanctions regulation.

4.4 Banks use the report format drawn-up by AFM and DNB to report a hit to the relevant supervisory authority. The DNB assesses the reports received from banks. In the event of a genuine hit, the DNB forwards the report to the Ministry of Finance. If the DNB believes, in assessing the report, that it is not a hit, the report is not forwarded to the Ministry of Finance. In both cases the reporting bank is advised accordingly.

Exemptions are possible in some cases (this may vary depending on the sanctions regulation). The Minister of Finance is authorised to decide on this. A substantiated request for exemption can be sent to the Ministry of Finance.

Where a bank freezes assets on the basis of a match with the 'terrorist lists', the bank must also look at the client's transaction history to see whether any transactions have occurred that may have been made in connection with TF. In case of a suspicion of TF, the bank must report those transactions to the FIU, in accordance with the Wwft.

Assets must remain frozen until the relevant sanctions regulation is changed and the obligation to freeze the assets is lifted, or an exemption is granted, or, if notice to the contrary is received from the Ministry of Finance or from 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.

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 filing a SAR, 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 its 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, the bank is open to prosecution.

Chapter 5

Staff screening, awareness and training

Wwft 35

5.1 One of the most important controls in the prevention and detection of ML/ TF is to have staff who is alert to the ML/ TF risks, well-trained in the identification of unusual activities or transactions which may be suspicious, and able to execute the appropriate CDD measures.

5.2 In 2020, an amendment to article 35 of the Wwft was introduced and accepted, which stipulated that staff and the day-to-day policymakers should be screened (in Dutch *worden doorgelicht*). This provision originates from article 8 of the EU AML/ CTF Directive.

In the Netherlands, banks are already subject to an obligation contained in article 13 of the Prudential Rules Decree Wft which states that an institution must make a substantiated assessment of the properness of individuals whom they wish to appoint to any integrity sensitive position. This forms the basis of the pre- and in-employment screening of staff.

The Prudential Rules Decree WftDecree gives institutions the option to decide which positions are integrity sensitive and require screening. In the absence of specific guidance on which position are integrity sensitive, most banks have decided to screen the majority of their employees. For these banks the introduction in article 35 of the Wwft does not bring a change. Banks who in the past have opted for a more restricted list of integrity sensitive postions should check whether all employees engaged in CDD processes have an integrity sensitive position and and should ensure that they are screened if that is the case in accordance with the applicable procedures for such positions.

5.3 The effective application of even the best-designed control systems can be quickly compromised, if the relevant staff applying the systems is not adequately trained. The content and effectivenesss of such training is therefore important to the success of the bank's AML/ CTF strategy. Paragraphs 5.3 to 5.17 are best practices for setting up and executing training and awareness activities, in line with the requirements of Wwft article 35.

5.4 Banks must implement a clear and well-articluated policy to ensure that the relevant staff is aware of their obligations in respect of the prevention of ML/ TF. Banks must also provide regular and relevant training to their staff (incl. senior management up to the highest level of the bank, temporary- and contract staff, and day-to-day policymakers (in Dutch *dagelijks beleidsbepalers)*), to allow them to obtain the knowledge and skills required to comply with their obligations and must train them in the identification and reporting of anything that gives grounds for suspicion. Banks must especially ensure that the staff (incl. temporary and contract staff) who directly handles customer transactions or instructions is trained.

5.5 In determining the nature and extent of AML/ CTF training measures, banks must take into consideration the nature and size of their businesses and the nature and the extent of the ML/ TF risks their business is subjected to.

5.6 Adequate training must be offered to all relevant employees (incl. (senior) management up the highest level of the bank) in order to enable them to obtain the knowledge and skills necessary for compliance with the obligations in respect of the prevention of ML/ TF. Banks should tailor the content, the technical level and frequency of training to the function of the staff (incl. senior management).

5.7 Banks must train their staff on how products and services may be used as a vehicle for ML/ TF, as well as on the bank's procedures for managing these risks.

5.8 Banks must futher train their staff in order to carry out their particular role. E.g., staff involved in customer acceptance, risk assessment, customer servicing, or having settlement functions needs different training, tailored to their particular function; and training to identify SARs that may involve ML/ TF is especially important for staff who directly handles customer transactions or instructions.

5.9 If the day-to-day policy of a bank is determined by two or more persons, the bank should designate a single person to be responsible for the bank's compliance with the provisions of the Wwft. This *'day-to-day Wwft policymaker'* must be aware of the bank's integrity-policy and of its procedures. They should also get periodically (demonstrably) adequate training regarding the Wwft.

5.10 Relevant staff also need to be made aware of the particular circumstances of customers who present a higher ML/ TF risk and of how best to identify these risks. Training must include how customer identity should be verified in such cases, what additional steps can be taken, and what (local) check can be made.

5.11 Staff awareness and training programs also include the nature of the TF and of the terrorist activity, in order that staff is alert to customer transactions or activities that might be terrorism-related.

5.12 Banks must make their staff aware of changing behavior and practices amongst money launderers and among financers of terrorism – e.g. the FATF typology reports.

5.13 Banks may use one or more training techniquesto train their staff – e.g.:

- online learning systems can often provide an adequate solution for the majority of the staff;
- focused classroom trainings may be more effective for higher-risk or minority areas.

5.14 In order to keep abreast of new developments and to continuously promote awareness of their staff, banks should offer training courses not offered, but regularly. Banks should give ongoing training at appropriate intervals to all relevant staff (incl. senior management), and should tailor this training to their functions. In larger banks, this ongoing training can take th form of a rolling programme.

5.15 Banks should keep trainings relevant and up-to-date and should evaluate and revise trainings on a regular basis.

5.17 Senior management of the bank must be (made) aware of the fact 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 (i.e. “willful blindness”).

Banks must inform their staff that they might be held personally liable for claims by third parties for damages caused by filled SARs or by information provided to supervisory authorities, if it is afterwards determined that (based on the facts and

circumstances) the SAR or the information should not have been provided to the authorities.

5.18 Finally, whatever the approach banks take to training their staff, they must establish comprehensive records to monitor who was trained, when they received the training, the nature of the training, and its effectiveness. Record keeping is also important for evaluating and revising trainings.

Chapter 6

Record Keeping

Core obligations

6.1 Banks must retain:

- All data, documentation and information obtained during the CDD process (e.g. copies of, or references to the evidence they obtained of a customer's identity) in order to satisfy their CDD obligations, for five years after the end of the customer relationship;
- Details of customer transactions, for five years from the date of the transaction;
- Details of actions taken in respect of internal and external SARs;
- Details of information considered by the relevant officer in respect of an internal SAR where no external report is made;
- Data regarding transactions which have been reported tot the FIU.

6.2 Banks must be aware of the fact that data, documentation and information recorded and stored in the context of fulfilling their CDD obligations contain personal data. This means that the GDPR provisions apply to these data, documentation and information. Banks must delete any personal data gathered as part of their CDD obligations and personal data relating to customer transactions, upon expiry of the retention period, unless otherwise prescribed by law.

6.3 Banks must maintain appropriate systems for retaining records and for making records available, upon demand, within specified timelines.

General legal and regulatory requirements

Wwft 33, 34

6.4 Banks are responsible for developing their own record retention policies and procedures according to the nature of their business.

6.5 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 in order 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 2b, 2f

6.6 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 record-keeping practices must be appropriate to the scale, nature and complexity of their business.

6.7 Banks must also document their risk assessments (e.g. SIRA) and their Group-wide policies, controls and procedures (incl. policies and procedures regarding data protection and sharing information, with the purpose to prevent ML and TF, within the Group).

Wwft 10

6.8 When a bank structurally oursources the application of CDD measures to a third party, the bank is also required to have written arrangements relating to the data retention practices it expects from that third party.

General records to be kept by banks

Wwft 33, 34, 35

6.9 The bank's records should cover information related to the bank fulfilling its AML/ CTF and Sanctions obligations in the following areas:

- Customer information;
- Transactions;
- Screening and monitoring records;
- Internal and external reports;
- Compliance monitoring/testing;
- Training and awareness.

Customer information

Wwft 33

6.10 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 its CDD obligations under the Wwft.

6.11 A bank may often hold additional information with respect to a customer, that be bank obtained for the purposes of EDD or for ongoing monitoring of the customer.

6.12 The customer file should also reveal how the decision-making process surrounding the acceptance of the customer has taken place (e.g. in the case of high-risk customers).

Wwft 33 (3)

6.13 Customer 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(s), or after the occasional transaction was carried out).

Wwft 34a(3)

6.14 Upon the expiry of the five-year retention period, 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.

A bank, as proof of the identification requirement (duty to reproduce), can document a copy of the verified identity document.[76] Based on the Wwft, Article 33, there is no requirement to document the citizen service number (in Dutch *burgerservicenummer*).

6.15 Where documents verifying the identity of a customer are held in a repository of one entity of a Group, they do not need to be held in duplicate form in another repository. The records do, however, need to be made easily accessible to all staff that have contact with the customer, and to be made readily available to supervisory authorities and law enforcement upon request. The data can be stored electronically or as a physical document.

6.16 When an introducing branch or subsidiary of a Group ceases to trade or to have a relationship with a customer, particular care needs to be taken to retain, or hand over, the appropriate customer records to other Group members, if the latter continue to have a relationship with the customer. Similar arrangements need to be made if a company holding relevant records ceases to be part of the Group, or the bank terminates a contract with a third party delegated to keep relevant records.

.....

[76] See the Guidelines 'Identification and verification of personal data' of the Dutch Data Protection Agency (In Dutch *Autoriteit Persoonsgegevens*)

Transactions

EU Regulation 2015/847 on information accompanying transfers of funds, 16

6.17 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, or cheques) must be maintained in a form from which allows a satisfactory audit trail to be compiled.

EU Regulation 2015/847 on information accompanying transfers of funds 16

6.18 Records of all transactions relating to a customer must be retained for a period of five years from:

- The date when the transaction is completed (where the records relate to an occasional transaction); or
- 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

6.19 Upon the expiry of the period referred to in paragraph 6.15, 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.

Wwft 34

6.20 A bank must make and retain:

- Records of actions taken under the internal and external SAR filing; and
- When the relevant officer has considered information or other material concerning possible ML/ TF, but has not filed a SAR to the FIU, a record of the other material that was considered.

6.21 In addition, copies of any SARs made to the FIU must be retained, incl.:

- 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.

6.22 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

6.23 A bank's records may consider:

(a) In relation to training:
- Dates of training;
- The nature of the training, and the involved staff;
- The results of the tests undertaken by staff, where appropriate.

(b) In relation to compliance monitoring:
- Reports by the relevant officer to senior management; and
- Compliance monitoring plans.

Wwft 33 (4)(5)

6.24 A bank must establish and maintain data retention systems wich enable it to respond fully and rapidly to inquiries from the FIU and/ or from the supervisory authorities, incl.:

- whether the bank maintains, or has maintained a customer relationship with a specific customer during the previous five years;
- what the nature of that customer relationship was.

6.25 The data retention systems should have secured channels that ensure the confidentiality of the inquiries of the FIU and/ or the supervisory authorities and the dated provided.

Form in which records have to be kept

6.26 Most banks have standard procedures that they keep under review and seek to reduce the volume and density of records that have to be stored, whilst still complying with the Wwft requirements. Retention may therefore be:

- By way of original documents;
- By way of photocopies of original documents;
- On microfiche;
- In scanned form; or

- In computerised or electronic form.

6.27 The record retention requirements are the same, regardless of the format in which data is kept, or whether the transaction was undertaken by paper or by electronic means.

6.28 Banks involved in mergers, take-overs or internal reorganisations need to ensure that records of identity verification and of transactions are readily retrievable for the required periods, when rationalizing computer systems and physical storage arrangements.

Location

6.29 The Wwft does not state where relevant records should be kept, but requires that banks are able to retrieve the relevant information, without undue delay.

6.30 Where identification records are held outside the Netherlands, it is the responsibility of the Dutch bank to ensure that the records meet the Wwft requirements. No secrecy or data protection legislation should restrict access (freely or upon request) to the records of the Dutch regulated bank, or by Dutch law enforcement agencies under court order or under relevant mutual assistance procedures. If the Dutch bank finds that such restrictions exist, the Dutch bank should request and retain (within the Netherlands) copies of the underlying records of identity.

6.31 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.

6.32 In case of tensions between the provisions of the Wwft and of the data protection legislation, the relevant officer has to balance both sets of obligations.

6.33 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 their 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 AML/ CTF legislation, and retaining electronic/ digital copies may be a more realistic storage method.

Sanctions and penalties

6.34 Where the record-keeping obligations under the Wwft are not observed, a bank or person is open to prosecution, including imprisonment, 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.

Chapter 7

Customer Tax Integrity

7.1 Legal framework

General

7.1.1 The statutory obligation of banks to ensure ethical operational management and to prevent involvement in ML/ TF must also be geared towards addressing customer tax integrity (hereinafter CTI) risks. There is a link between ML and illegal and/ or harmful tax practices.

Wwft 3(10) and DNB Good Practices: Customer Tax integrity, Chapter 2

7.1.2 CTI should form part of the overall risk-based approach a bank takes to protect itself from being used by customers to commit the crime of tax evasion (which is a predicate offence for ML), or to engage in aggressive tax avoidance.

7.1.3 A bank should establish a clear decision tree and escalation path when determining their CTI risks. Such a decision tree should involve the First Line, Compliance and the Tax department. When designing measures to mitigate CTI risks banks should, among others, implement mechanisms for the monitoring and escalation of red flags, and should execute appropriate training and awareness.

7.1.4 This chapter should be read in conjunction with Chapters 1, 2, 3 and 5 of this Guidance.

The concept of CTI

7.1.5 The CTI risks are in essence a derived risk for banks. It is the risk that the bank becomes involved in the commission of illegal and/ or harmful tax practices by their customers – incl. tax evasion and aggressive tax avoidance (also known as aggressive tax planning).

7.1.6 Tax evasion can be understood as the illegal non-payment or underpayment of taxes, and is a predicate offence for ML – e.g. the (intentional) establishment of offshore constructions by a private individual or legal entity with the goal to disguise ownership and/ or control, leading to non-adherence to applicable laws regarding tax liability.

7.1.7 Aggressive tax avoidance is a more open and less defined practice. It consists in taxpayers' reducing their tax liability through arrangements that may be legal, but that are in contradiction with the intent of the law. The difference with tax evasion is that aggressive tax avoidance is not illegal. It does, however, have harmful effects and social tolerance is decreasing. A bank's involvement in these practices could damage the bank's reputation and erode the public's trust in the financial sector, as a whole.

7.1.8 CTI risks and illegal and/ or harmful tax practices exclude acceptable tax planning. The latter is the use of tax incentives, as intended by the law.

Regulatory framework

7.1.9 Public and political scrutiny of tax arrangements of multinational companies and high net-worth individuals has led to profound international tax changes in the context of the OECD Base Erosion and Profit Shifting (BEPS) project. The effects of these international developments are increasingly finding their way into the local financial regulatory environment.

7.1.10 In this Chapter, reference is specifically made to the following documents and legislation:

- The DNB Good Practices Customer Tax Integrity Risk Management, July 2019 (hereinafter DNB Good Practices);
- The EU Directives on Administrative Cooperation.

7.2 Risk assessment (refer to Chapter 1)

7.2.1 CTI must form an integral part of a bank's risk-based approach. This includes, but is not limited to, ensuring CTI is taken into account in:

- The Risk Appetite Statement (both inclusion and exclusion areas);
- The SIRA and in any other specific risk assessments;
- The Country risk ratings (e.g. by taking into account jurisdictions considered by the EC as non-cooperative for tax purposes);
- The identification of higher-risk corporate structures and of any other relevant risk category or factor.

7.2.2 Banks should assess and monitor CTI risks at the customer, transaction, product and employee behaviour levels.

7.3 Risk assessment – identification and assessment of business risks (refer to Chapter 1.3)

DNB Good Practices, Chapter 3

7.3.1 A bank must ensure that CTI risks are incorporated into integrity exercises – e.g. the SIRA. In the SIRA, a bank must identify scenarios relating to risks of tax evasion and of aggressive tax avoidance, leveraging the high-risk indicators it has identified for its various business segments.

7.3.2 A bank should be able to demonstrate where in its portfolio it has assessed CTI risks to be higher, and why. To facilitate this, a bank may consider creating a comprehensive overview, either overall or CTI-specific, based on risk levels assigned to customer categories, activities, domiciles, sectors, etc. This would assist in any periodic, or holistic evaluation of risk concentration, and may help a bank to establish limits per customer segment and per business sector, as part of its risk appetite.

7.3.3 Whether overarching, as part of a multidisciplinary approach, or CTI-specific, a bank should conduct periodic portfolio level scans to identify customer concentrations or product exposures requiring additional measures under a risk-based approach.

7.4 A risk-based approach – customer risk assessments (refer to Chapter 1.5)

7.4.1 When performing a risk assessment of the customer which includes CTI, a bank may, among other measures, be guided by the following:

- Residence substance:
  - For entities: examine the place of effective management and assessment of the complexity of the ownership and control structure
  - For individuals: examine the center of their social/ daily life
- Economic rationale: This test is performed in order to establish economic rationale/ substance of a customer -e.g. does the company perform operational or investment activities or is it a so-called shell company (such company has no physical presence (other than a mailing address) and generates little to no economic value).
- Transparency: This test is performed in order to examine the level of transparency the customer exercises toward the bank.

7.4.2 Banks should consider to include the risk that an employee willingly facilitates illegal and/ or harmful tax practices by customers in their risk assessments for CTI.

7.5 Application of CDD Measures (refer to Chapters 2.3 and 3)

DNB Good Practices, Chapters 3, 5

7.5.1 CTI must be an integral part of any risk-based CDD end-to-end process, as described in Chapter 2. This, for example, includes getting an understanding of the ownership and control structure and establishing, monitoring, and reviewing transaction monitoring scenarios.

7.5.2 CTI risk must be specifically taken into account as part of the CDD process (incl., where applicable, EDD measures) whenever a red flag is observed. An example of a CDD-related red flag for CTI may be companies located in offshore countries. Tax-related adverse name and media alerts should always be included among the red flags for CTI. When doing so, a bank must ensure access to appropriate tax expertise, whether internal or external, as well as a clear decision tree and escalation path

7.5.3 As with ML/ TF and Sanctions, to understand CTI risks posed by a customer, identification and verification of the ownership and control structure is required in order to obtain full information on the UBO(s), gaining insight in the private individuals or entities that own or control the customer, and/ or gaining insight into who ultimately has the benefit of the revenues of that customer.

7.6 Monitoring customer activity (refer to Chapter 2.7)

Transaction Due Diligence

7.6.1 This section refers to risk assessments that should be performed during due diligence for transactions which are not payment transactions. Those are covered by Post-Event Transaction Monitoring below.

DAC6

7.6.2 A bank should assess and address tax evasion and aggressive tax avoidance risks before engaging in or facilitating a transaction, as well as whether or not the deal may be reportable under DAC6, where the bank is considered an intermediate for DAC6.

7.6.3 To identify whether such a risk exists, the following examples of red flags/ high risk indicators may be considered:

- The transaction lacks economic substance/ rationale;
- The transaction involves a customer with a complex ownership and control structure;

- The fee/ income is linked to the tax benefit generated by the transaction;
- The transaction relates to a major restructuring of the business activities of the customer;
- The transaction involves the use of a non-transparent legal or beneficial ownership structure.

Post-event Transaction Monitoring (PTM)

DNB Good Practices, Chapters 5, 6

7.6.4 A bank maintains expected payment transaction profiles for its customers based on information provided by the customer. When defining these profiles and for monitoring purposes, a bank should take CTI into consideration.

7.6.5 A bank must develop and periodically assess specific PTM scenarios and business rules with respect to tax integrity risks for detecting unusual or higher-risk payment transactions. Such scenarios for tax evasion and aggressive tax avoidance should be based at least in part on the bank's existing customer portfolio and back testing of previously assessed files.

7.6.6. Any payment transactions for which red flags are triggered, and which are not consistent with the purpose and nature of the relationship (refer to expected customer behaviour in Chapter 2.8.4), the customer's risk profile, as well as the products and services offered to the customer should trigger a risk assessment that incorporates CTI. A bank must ensure the appropriate levels of training for and expertise of employees in performing such assessments.

7.7 Product Risk

DNB Good Practices, Chapter 3

7.7.1 In line with the bank's risk appetite, a bank should assess each product to ensure it does not knowingly and actively facilitate tax evasion or aggressive tax avoidance by customers. The triggers for product risk assessments should be (a) any new product; and (b) any product subject to a review cycle.As with customer and transaction risk assessments, the appropriate level of tax expertise must be ensured to appropriately assess the tax impact of each new product or product in review, assessing the risk that the product can be used for the active facilitation of tax evasion or aggressive tax avoidance by customers.

7.8 Employee Conduct Risk

7.8.1 As part of a risk-based approach, a bank should take proportionate measures to mitigate the risk of employees facilitating tax evasion or aggressive tax avoidance. This includes identifying those employees with a higher facilitation risk, delivering appropriate training and establishing any necessary controls. Refer to Staff Awareness & Training.

7.8.2 As part of its risk assessments, a bank should adequately identify the risk that an employee willingly and knowingly facilitate customer tax evasion or aggressive tax avoidance.

7.8.3 A bank may wish to consider including reference to the facilitation of unacceptable tax behaviour in its relevant code of conduct, and/ or any other similar documentation concerning culture, ethics and values.

7.9 Staff awareness and training (refer to Chapter 5)

Training

DNB Good Practices, Chapter 6

7.9.1 A bank should issue CTI trainings, which should be tailored to the staff's role. While bespoke training should be provided to those in higher-risk positions (e.g. alert and hit handlers, MLROs, as well as staff representing an elevated risk for facilitation), other staff may benefit from a more generic training. Such generic training may be part of a wider training provided on ML/ TF, etc., and/ or which also makes reference to risk of facilitation of fraud or of unacceptable behaviour, more generally.

Demonstrating staff awareness

7.9.2 For staff awareness on CTI, a bank should be able to evidence:

- That Senior Management owns and understands CTI risk and advocates the measures designed to prevent the bank from being used to facilitate tax evasion or aggressive tax avoidance;
- That relevant employees have been trained on, and are aware of, CTI and of the responsibilities of the bank in this regard;
- That incident management procedures (e.g. whistleblowing) are referenced to in communication to emphasize the channels available to report any suspicious or unacceptable behaviour.

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 private individuals 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/ ATF and Sanctions	DNB Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act an the Sanctions Act
Entity	An entity is not a private individual and can establish a permanent customer relationship with the bank or otherwise own property – e.g. limited liability companies, (private/ limited) partnerships, trusts or other similar legal arrangements.
EU Sanctions Regulation	Regulation 2580/2001, on specific restrictive measures directed against certain persons and entities with a view to combating terrorism.
European Economic Area (EEA)	Member States of the European Union, plus Iceland, Liechtenstein and Norway.
EVA, SFH and VIS	Systems used by financial instutions to check if a person is listed in internal or external (referral) registers
Event	An event is defined as a change in the customer data or in the 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.
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 EU/EEA Member State; 2. a firm mentioned in article 1a (4)(f) Wwft who has a licence 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 EU/EEA 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 EU/EEA 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.
Group	A Group is composed of a bank and one or more direct or indirect subsidiaries and/ or entities in which the bank has a stake of more than 50 per cent and/ or management control.
Identification	Ascertaining the name of, and other relevant information about, a customer or beneficial owner.
Legal representatives	Those individuals who, individually or collectivelyrepresents or stands in the place of another under authority recognized by law
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 organised 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, incl. PSPs and administrators and exchanges of virtual currencies (e.g. Bitcoin). *[Article 1.1 Wft]*
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 their identity from the authorities.
Non-transparant country	Non-transparent countries 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 countries 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]*
Offshore countries	Countries with financial centres that contain financial institutions that deal primarily with nonresidents and/or in foreign currency on a scale out of proportion to the size of the host economy
Ownership interest	Any transaction that is not carried out as part of a customer relationship.
Relevant related party	Relevant related parties to entities include but are not limited to: • UBOs; • Holders of power of attorney (such as authorised agents); • Legal representatives; • Authorised representatives; • Guarantors; • Beneficiaries of a product. Relevant related party to a private individual include but are not limited to: • Holders of power of attorney (such as authorised agents); • (Legal) representatives; • Guarantors; • Beneficiaries of a product (e.g. life insurance payments). *[Article 3 lid 5 sub b and g Wwft]*
Risk factor	A variable that, either on its own or in combination, may increase or decrease the ML/TF risk posed by an individual customer relationship or occasional transaction.
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, UBO 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 private individual who is known to have joint beneficial ownership of legal entities or legal arrangements; (ii) any private individual 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. Customers 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 Regulated Entity	A financial institution that is regulated by a regulator from EU/EEA Member States or a country with an equivalent AML/CTF system (the Recognised Regulators List).
Recognised Regulators List	A financial institution's approved list of supervisory authorities from EU/EEA Members and from countries that it considers having an equivalent AML/CTF system to the EU.
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)]*
Relevant officer	A person in a bank or organisation which has the task to file reports to the Financial Intelligence Units. This specific role/functions of this person can vary per country. Based on article 2d (2)(3) Wwft the person with a compliance function files reports to the FIU in the Netherlands.
Senior management of the bank	Senior management of a bank in the context of approval for entering and/or continueing a customer relationship (customer or UBO is PEP, EC high-risk third countries and correspondent relationships) are: a. persons who determine the day-to-day policy of an institution; or b. persons working under the responsibility of a bank, 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 ML/TF risk exposure of a bank. *[Article 1.1 Wwft]*
Senior managing official of a customer (*hoger leidinggevend personeel*)	In the context of pseudo-UBOs, Senior managing officials are defined as: a. The statutory board of a customer, meaning all the board members. In case of a one tier board this includes the executive board members and also the non-executive board members. b. All the partners of a partnership (except the silent partners).
SFH	See EVA

Shell company	A company that is incorporated that have no significant operations or related assets, often set up in offshore countries.
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 private individual i.e. those activities that have generated a person's net assets and property.
State-owned enterprises	Profit enterprises where the state has ownership of greater than 50% and/or where information reasonably available points to the state having control over the activities of such enterprises.
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]*
Tipping off	A tipping-off offence is committed, if an individual knows or suspects that a disclosure falling under Article 15 Wwft and Annex Indicators Uitvoeringsbesluit Wwft 2018 has been made, and 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 private individual (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.
VIS	See EVA

Abbreviation

AFM	Autoriteit Financiële Markten
AML	Anti-money laundering
BV	Besloten Vennootschap (public limited company)
CITES	Convention on International Trade in Endangered Species of Wild Fauna and Flora
CTF	Combating terrorist financing
CTI	Customer tax integrity
DNB	De Nederlandse Bank (Dutch Central Bank)
EBA	European Banking Authority
EC	European Commission
EDD	Enhanced Due Diligence
ESA	The European Supervisory Authorities (The European Banking Authority, the European Securities Markets Authority and the European Insurance and Occupational Pensions Authority, working together)
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
GDPR	General Data Protection Regulation
IMF	International Monetary Fund
IWT	Illegal wildlife trafficking
JMLSG	Joint Money Laundering Steering Group (UK)
MiFID	The Marketing in Financial Instruments Directive
ML	Money Laundering
NV	Naamloze Vennootschap (public limited company)
NVB	Nederlandse Vereniging van Banken (Dutch Banking Associaton)
OFAC	The Office of Foreign Assets Control

PEP	Politically Exposed Person
PSP	Payment Service Provider
SDD	Simplified Due Diligence
SIRA	Systematic Integrity Risk Analysis
STAK	Stichting Administratie Kantoor
SW	Sanctiewet 1977
TF	Terrorist Financing
UAVG	Uitvoeringswet Algemene verordening gegevensbescherming (Implementing Act of the General Data Protection Regulation)
UN	United Nations
WED	Wet op de Economische Delicten
WFOE	Wholly foreign-owned enterprise
Wft	Wet op het financieel toezicht
Wtt	Wet op de trustkantoren (Trust Offices Supervision Act)
Wwft	Wet ter voorkoming van witwassen en financieren van terrorisme

Annex I - List of Recognised Exchanges

Methodology

The following methodology is applied for the selection of countries with an adequate transparency regime to be listed on the List of Recognised Exchanges.

EU/EEA Member States

According to the Implementing Decree Wwft 3(1a), banks are not obliged to identify UBO(s) of companies (including (in)direct 100% subsidiaries) listed on a regulated market, that is subject to disclosure requirements consistent with EU law, or subject to equivalent international standards, which ensure adequate transparency of ownership information. As all EU/ EEA Member States are obliged to implement the Directive 2004/109/ EC.[77] The regulated markets of the EU/EEA Members States are considered to have appropriate standards in place to ensure adequate transparency of ownership information. These transparency requirements relate to all major holdings of shares or other financial instruments as referred to in Directive 2004/109/EC and not only to the number of shares or financial instruments available to the public for trading in the secondary market (free float).

OECD Corporate Governance Factbook

The OECD Corporate Governance Factbook was published for the first time in 2014 and is updated regularly.[78] Based on 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, Costa Rica, Hong Kong, India, Indonesia, Israel, Japan, Korea (South), Malaysia, Mexico, New Zealand, Singapore, South Africa, Turkey and United States.

Additional countries

Additional countries can be added to the list after it has been determined that the concerned country meets the criteria listed below. These requirements are derived from Directive 2004/109/EC. Banks must perform this assessment based on relevant and current data and information. This 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 articles 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 of the enterprises it controls.

.....

[77] Directive 2004/109/EC on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market, available at bit.ly/3bjrjA5.

[78] OECD. Corporate Governance Factbook – 2019, available at bit.ly/3pBykBs.

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 identification of the shareholder, the dates of the change and the voting threshold achieved. The information should be made public, without delay, by the issuer or by 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	Bolsas y Mercados Argentinos	www.merval.sba.com.ar
Australia	Australian Securities Exchange	www.asx.com.au
Austria	Wiener Börse	www.wienerborse.at
Belgium	Euronext Brussels	www.euronext.com
Brazil	B3 - Brasil Bolsa Balcão S.A	http://www.b3.com.br/en_us/
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
Costa Rica	Bolsa de Valores de Costa Rica	www.bolsacr.com
Croatia	Zagreb Stock Exchange	bit.ly/3k6cdlt

Country	Exchange	Web address
Cyprus (Republic of)	Cyprus Stock Exchange	www.cse.com.cy
Czech Republic	Prague Stock Exchange	www.pse.cz
Denmark	Nasdaq Copenhagen A/S	www.nasdaqomxnordic.com
Estonia	Nasdaq Tallinn	www.nasdaqomxbaltic.com
Finland	Nasdaq Helsinki	www.nasdaqomxnordic.com
France	Euronext Paris	www.euronext.com
Germany	Deutsche Börse AG	www.deutsche-boerse.com
Greece	Athens Stock Exchange	www.helex.gr
Hong Kong	Hong Kong Exchanges and Clearing Limited (HKEX)	bit.ly/2NEInZ6
Hungary	Budapest Stock Exchange	www.bse.hu
Iceland	Nasdaq Iceland	www.nasdaqomxnordic.com
India	National Stock Exchange of India	www.nseindia.com
	Bombay Stock Exchange	www.bseindia.com
Indonesia	Indonesia Stock Exchange	www.idx.co.id/en-us
Ireland	Euronext Dublin	www.ise.ie
Israel	Tel Aviv Stock Exchange	www.tase.co.il
Italy	Borsa Italiana	www.borsaitaliana.it
Japan	Japan Exchange Group	www.jpx.co.jp
Korea, South	Korea Exchange (KOSPI)	www.krx.co.kr.
Latvia	Nasdaq Riga	www.nasdaqomxbaltic.com
Lithuania	Nasdaq Vilnius	www.nasdaqomxbaltic.com
Luxembourgh	Luxembourg Stock Exchange	www.bourse.lu
Malta	Malta Stock Exchange	www.borzamalta.com.mt
Malaysia	Bursa Malaysia	www.bursamalaysia.com
Mexico	Bolsa Mexicana de Valores	www.bmv.com.mx/en
Netherlands	Euronext Amsterdam	www.euronext.com
New Zealand	NZX Limited	www.nzx.com
Norway	Oslo Børs	www.oslobors.no
Poland	Warsaw Stock Exchange	www.gpw.pl
Portugal	Euronext Lisbon	www.euronext.com
Romania	Bucharest Stock Exchange	www.bvb.ro
Singapore	Singapore Exchange	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 Stockholm	www.nasdaqomxnordic.com
Switzerland	SIX Swiss Exchange	www.six-swiss-exchange.com
Turkey	Borsa Istanbul	www.borsaistanbul.com
United Kingdom	London Stock Exchange	www.londonstockexchange.com
United States	New York Stock Exchange	www.nyse.com
	NASDAQ US	www.nasdaqomx.com

Annex II - List of Recognised Regulators

Methodology

The following methodology applies for selecting countries with an adequate transparency regime to be listed on the List of Recognised Exchanges.

EU/EEA Member States

Banks may, according to article 5 sub 1a Wwft, rely on other financial institutions.

Equivalent countries

Next to EU/ EEA Member States, reliance may be placed on countries that apply CDD 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. Countries that are registered on the FATF list of High-Risk Jurisdictions subject to a call of Action are excluded from this list. Russia is excluded from this list due to the Ukraine-related sanctions imposed by the EU.

Country	Regulator	Web address
Argentina	Central Bank of Argentina	www.bcra.gob.ar
	Superintendencia de los Seguros de la Nación (SSN)	https://www.argentina.gob.ar/superintendencia-de-seguros
	Comisión Nacional de Valores (CNV)	https://www.argentina.gob.ar/cnv
Australia	Australian Prudential Regulation Authority	www.apra.gov.au
	Reserve Bank of Australia	www.rba.gov.au
	Australian Securities and Investments Commission	www.asic.gov.au
	Australian Transaction Reports and Analysis Centre	https://www.austrac.gov.au/
Austria	Austrian Financial Market Authority	www.fma.gv.at
	Österreichische Nationalbank	www.oenb.at
Belgium	Financial Services and Markets Authority	https://www.fsma.be
	National Bank of Belgium	www.nbb.be
Brazil	Commissão de Valores Mobiliários	www.cvm.gov.br
	Banco Central do Brasil	www.bcb.gov.br
	Superintendence of Private Insurance	www.susep.gov.br
Bulgaria	Financial Supervision Commission	www.fsc.bg
	Bulgarian National Bank	www.bnb.bg
	Financial Intelligence Directorate - State Agency for National Security (FID-SANS)	https://www.dans.bg/en

Country	Regulator	Web address
Canada	Office of the Superintendent of Financial Institutions	www.osfi-bsif.gc.ca
	Canadian Securities Administrators: • Alberta Securities Commission • Autorité des Marchés Financiers • British Columbia Securities Commission • Ontario Securities Commission	www.securities-administrators.ca/ www.albertasecurities.com lautorite.qc.ca www.bcsc.bc.ca www.osc.gov.on.ca
	Financial Services Commission of Ontario	www.fsco.gov.on.ca
	Investment Industry Regulatory Organisation of Canada	www.iiroc.ca
	Mutual Fund Dealers Association of Canada	mfda.ca
	Financial Transactions and Reports Analysis Centre of Canada	https://www.fintrac-canafe.gc.ca/intro-eng
Chile	Superintendencia de Bancos e Instituciones Financieras Chile	www.sbif.cl
	Superintendencia de Pensiones	
	Unidad de Análisis Financiero	www.uaf.cl
China	The People's Bank of China	www.pbc.gov.cn
	China Banking and insurance Regulatory Commission	www.cbirc.gov.cn
Colombia	Superintendencia Financiera de Colombia (Financial Superintendent of Colombia, SFC)	https://www.superfinanciera.gov.co/jsp/index.jsf
	Dirección de Impuestos y Aduanas Nacionales (National Tax and Customs Office, DIAN)	https://www.dian.gov.co/
	Ministerio de Tecnologías de la Información y las Comunicaciones (Ministry of Information and Communication Technologies, MINTIC)	https://www.mintic.gov.co/portal/inicio/
	Superintendencia de Economía Solidaria (Superintendent of Solidarity-based Economy, SES)	http://www.supersolidaria.gov.co/
Croatia	Croatian Financial Services Supervisory Agency	www.hanfa.hr
	Croatian National Bank	www.hnb.hr
	Ministry of Finance, Financial Inspectorate	https://mfin.gov.hr/en
Cyprus (Republic of)	Central Bank of Cyprus	www.centralbank.cy
	Cyprus Securities and Exchange Commission	www.cysec.gov.cy
	Insurance Companies Control Service (ICCS)	http://mof.gov.cy/en/directorates-units/insurance-companies-control-service
Czech Republic	Czech National Bank	www.cnb.cz
	Financial Analytical Office of the Czech Republic	https://www.financnianalytickyurad.cz/
Denmark	Financial Supervisory Authority	https://www.dfsa.dk/
	National Bank of Denmark	www.nationalbanken.dk

Country	Regulator	Web address
Estonia	Bank of Estonia	www.eestipank.ee
	Estonian Financial Supervision and Resolution Authority	www.fi.ee
	Estonian Financial Intelligence Unit	https://www.fiu.ee/en
Finland	Financial Supervision Authority	www.finanssivalvonta.fi
	Regional State Administrative Agency for Southern Finland	https://avi.fi/en/southern-finland
France	Banque de France	https://www.banque-france.fr/
	Autorité des Marchés Financiers	www.amf-france.org
	Autorité de Contrôle Prudentiel et de Résolution (Prudential Supervisory and Resolution Authority)	https://acpr.banque-france.fr/en
Germany	Bundesanstalt für Finanzdienstleistungsaufsicht	www.bafin.de
	Deutsche Bundesbank	www.bundesbank.de
Greece	Hellenic Republic Capital Market Commission	www.hcmc.gr
	Bank of Greece	www.bankofgreece.gr
Hong Kong	Hong Kong Monetary Authority	www.hkma.gov.hk
	Securities and Futures Commission	https://www.sfc.hk/en/
	Insurance Authority	https://www.ia.org.hk/en/index.html
Hungary	National Bank of Hungary	www.mnb.hu
Iceland	Icelandic Financial Supervisory Authority	www.fme.is
India	Reserve Bank of India	www.rbi.org.in
	Securities and Exchange Board of India	www.sebi.gov.in
	Insurance Regulatory and Development Authority of India	www.irdai.gov.in
Ireland	Central Bank of Ireland	www.centralbank.ie
Israel	Israel Securities Authority	www.isa.gov.il
	Bank of Israel	www.boi.org.il
	Capital Markets Insurance and Savings Authority	https://www.gov.il/he/departments/capital_market_authority
Italy	Banca d'Italia	www.bancaditalia.it
	Commissione Nazionale per le Società e la Borsa	www.consob.it
	Istituto per la Vigilanza sulle Assicurazioni	www.ivass.it
	OAM (Organismo degli Agenti e dei Mediatori)	https://www.organismo-am.it/
Japan	Financial Services Agency	www.fsa.go.jp
	Securities and Exchange Surveillance Commission	https://www.fsa.go.jp/sesc/
	Bank of Japan	www.boj.or.jp/en
Korea, South	Bank of Korea	www.bok.or.kr/eng
	Financial Supervisory Service	english.fss.or.kr
	Korean Financial Intelligence Unit (KoFIU)	https://www.kofiu.go.kr/eng/intro/about.do
	Financial Service Commission	https://www.fsc.go.kr/eng

Country	Regulator	Web address
Latvia	Financial and Capital Market Commission	www.fktk.lv/lv
	The Bank of Latvia	www.bank.lv
Liechtenstein	Finanzmarktaufzicht Liechtenstein	www.fma-li.li
Lithuania	Bank of Lithuania	www.lb.lt
Luxembourg	Central Bank of Luxembourg	www.bcl.lu
	Commission de Surveillance du Secteur Financier (CSSF)	www.cssf.lu
	Commissariat aux Assurances	https://www.caa.lu/
Malaysia	Bank Negara Malaysia (Central bank of Malaysia)	www.bnm.gov.my
	Labuan Financial Services Authority	www.labuanibfc.com
	Securities Commission of Malaysia	https://www.sc.com.my/
Malta	Central Bank of Malta	www.centralbankmalta.org
	Malta Financial Services Authority	www.mfsa.com.mt
	Financial Intelligence Analysis Unit (FIAU)	https://fiaumalta.org/
Mexico	Comisión Nacional Bancaria y de Valores	www.gob.mx/cnbv
	Banco de México	www.banxico.org.mx
	Comisión Nacional de Seguros y Fianzas	www.gob.mx/cnsf
	Comisión Nacional del Sistema de Ahorro para el Retiro	https://www.gob.mx/consar
Netherlands	De Nederlandsche Bank (DNB)	www.dnb.nl
	The Dutch Authority for the Financial Markets (AFM)	www.afm.nl
New Zealand	Reserve Bank of New Zealand	www.rbnz.govt.nz
	Financial Markets Authority	www.fma.govt.nz
Norway	Financial Supervisory Authority of Norway	www.finanstilsynet.no
	Central Bank of Norway	www.norges-bank.no
Poland	Polish Financial Supervision Authority	www.knf.gov.pl
	National Bank of Poland	www.nbp.pl
	The General Inspector of Financial Information (GIFI) (FIU Poland)	https://www.gov.pl/web/mswia/giif
Portugal	Comissão do Mercado de Valores Mobiliários	www.cmvm.pt
	Banco de Portugal	www.bportugal.pt/en
	Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF; Insurance and pension funds Supervisory authority)	https://www.asf.com.pt/
Romania	Romanian Financial Supervisory Authority National Bank of Romania	asfromania.ro/en www.bnro.ro/Home.aspx
Singapore	Monetary Authority of Singapore	www.mas.gov.sg
	Insolvency and Public Trustee's Office	https://io.mlaw.gov.sg/
Slovakia	National Bank of Slovakia	www.nbs.sk/en/home

Country	Regulator	Web address
Slovakia	Financial Intelligence Unit of the National Criminal Agency	https://www.minv.sk/?financna-policia
Slovenia	Bank of Slovenia	www.bsi.si/en
	Securities Market Agency	www.a-tvp.si
	Office of the Republic of Slovenia for the Prevention of Money Laundering	http://www.uppd.gov.si/en/
	Insurance Supervision Agency (AZN)	https://www.a-zn.si/en/
South Africa	South African Reserve Bank	https://www.resbank.co.za/
	Financial Services Board	https://www.fsca.co.za/Pages/Default.aspx
Spain	Banco de España	www.bde.es/bde/es
	Dirección General de Seguros y Fondos de Pensiones	www.dgsfp.mineco.es
	Comisión Nacional del Mercado de Valores	www.cnmv.es
	Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (Sepblac)	https://www.sepblac.es/en/
Sweden	Finansinspektionen	www.fi.se
	Sveriges Riksbank	www.riksbank.se/en-gb
Switzerland	Swiss National Bank	www.snb.ch/en
	Swiss Financial Market Supervisory Authority	www.finma.ch
	All OARs recognised by and mentioned on FINMA website	https://www.finma.ch/en/finma-public/authorised-institutions-individuals-and-products/
Turkey	Central Bank of the Republic of Turkey	www.tcmb.gov.tr
	Banking Regulation and Supervision Agency (BRSA)	www.bddk.org.tr
	Capital Markets Board (CMB)	https://www.cmb.gov.tr/
	Financial Crimes Investigation Board (MASAK)	https://en.hmb.gov.tr/fcib-presentation
United Kingdom United Kingdom	Bank of England	www.bankofengland.co.uk
	Prudential Regulatory Authority (PRA)	https://www.bankofengland.co.uk/prudential-regulation
	Financial Conduct Authority	www.fca.org.uk/
	Her Majesty's Revenue and Customs (HMRC)	https://www.gov.uk/government/organisations/hm-revenue-customs

Country	Regulator	Web address
United States (In addition each state has its own supervisory authorities)	Board of Governors of the Federal Reserve System	www.federalreserve.gov
	Federal Deposit Insurance Corporation	www.fdic.gov
	National Credit Union Administration	www.ncua.gov
	National Futures Association	www.nfa.futures.org
	U.S. Commodity Futures Trading Commission	www.cftc.gov
	Office of the Comptroller of the Currency	www.occ.treas.gov
	Security & Exchange Commission	www.sec.gov
	Financial Crimes Enforcement Network	www.fincen.gov
	Financial Industry Regulatory Authority	www.finra.org
	New York State Department of Financial Services	www.dfs.ny.gov

Annex III - List of high risk sectors

Introduction

Customers can be active in a risk enhancing sectors. A bank assess the sector risk for each customer and, if necessary determines the measures that needs to be taken to mitigate the increased risk. This annex contains a list of high risk sectors. Per high risk sector a rationale and the type of risk has been set out.

Please note that this is a non-exhaustive list. Each bank can have additional sectors, that based on bank-specific indicators, are appointed as a high risk sector. For example based on the risk appetite or the profile of the bank.

Sources taken into account for the list of high risk sectors

The following sources have been taken into account when establishing the list of high risk sectors:

- Dutch Anti-Money Laundering and Counter-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme: Wwft)
- Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amended by Directive (EU) 2018/843
- The EU Supranational Risk Assessment on ML and TF (2019)
- The Dutch National Risk Assessment on ML (2019)
- The Dutch National Risk Assessment on TF (2019)
- DNB Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act (2019)
- DNB Good Practices: Customer tax integrity risk management (2019)
- DNB: Good practices Fighting Corruption (2014)
- Dutch Ministry of Finance Guidance on the Wwft (2020)
- FATF Recommendations and guidance papers
- EBA Revised Guidelines on ML/TF risk factors (2020)

Sector	Rationale	Risk
Oil, natural gas, energy, raw materials, minerals, mining	This sector involves contract (tenders/permits) with governments and possible PEP-involvement. Therefore this sector has a higher risk of corruption and bribery. In some countries with a lack of effective government control of territory and its resources, the natural resource sector may be vulnerable to exploitation for TF. There can also be sanctions related to this sector and sanctions on specific key players in this sector.	ML Corruption Sanctions TF Tax

Sector	Rationale	Risk
Loose diamonds traders & precious metals traders	Diamonds have characteristics (e.g. small, high value, easy to take along) that make them suitable to be used in the process of money laundering. They are easily smuggled and traded. In addition diamonds can also be obtained by modern slavery. The precious metal sector is high risk sector due to the fact that precious metals are a form of global currency and act as a medium for exchange in criminal transactions. Precious metals are also easily smuggled and traded (both physically and virtually) and have a high value..	ML TF
Jewellers, art dealers, auction houses, traders in luxury/valuable products including ships)	Due to the high value of the goods sold by this sector there is a higher risk of ML. The purchase of value goods is typical for the integration phase of ML. By purchasing high value goods, criminal proceeds can be integrated in the financial system.	ML
(Online) gambling	This sector can be used in the process of ML, when illicit proceeds (for example cash) is changed into proceeds with a potential legitimate origin. With regards to online gambling, the source/origin of the funds used/deposit can be difficult to establish (for example due to the use of prepaid-card or third party accounts).	ML
Trust and Company Service Providers (TCSP) (including trust services) and object companies & conduit companies serviced by trust offices	TCSPs are used to set up complex (international) organizational structures. These structures can be used to conceal the beneficial ownership of the customer/organization or for tax purposes. In these structures object companies and conduit companies are often used. Within the Netherlands, trust offices are subject to supervision. However some offices split their services with the purpose to no longer be subject to the supervision.	ML Tax
Commercial real estate	This sector brings a higher risk of ML. There are multiple ways in which this sector can be used for ML. For example via ABC-transactions, loan back constructions, concealment of the ownership of the property or due to an unknown origin of the funds used to buy the property.	ML Corruption Tax
Coffee shops	In some countries, for example the Netherlands, it is allowed to sell cannabis via coffee shops. However the purchase of the cannabis by the coffee shops is illegal. As a result of this being illegal, there is a criminal interference of this sector. In addition also the harvest of cannabis is illegal. Due to the fact that a lot of the transactions in this sector are cash, the origin of the funds can be hard to establish.	ML

Sector	Rationale	Risk
Grow shops	Grow shops are an important element in the production chain of cannabis. When the materials are sold for professional harvesting of cannabis, this is illegal.	ML
Cash-intensive businesses	The use of cash brings a higher risk. Cash conceals the origin of the funds and therefore there is a higher risk of ML.	ML
Sex industry / adult entertainment	This sector can be related to illegal (prostitution) activities, such as human trafficking. In addition this sector is also vulnerable to ML because of the amount of cash often used in this sector.	ML
Virtual Assets Service Providers (VASP)	Virtual assets can be used in the ML process. A virtual currency transaction can have more anonymity than for example a bank wire transfer. Therefore it can be difficult to establish the origin of the funds and the final destination of the funds. As a result of the latter, this sector also has a higher risk of TF	ML TF
Military goods, defence industry	This sector has multiple risk. Often contracts with governments (and PEPs) are involved, this results in a higher risk of corruption. There is also a higher risk on TF due to the possible illegal sale of weapons to terrorist. Due to sanction restriction on several of goods related to this sector, there is also a higher risk on sanctions.	Corruption Sanctions TF
Religious institutions and charities (foundations)	One of the biggest terrorist financing threats in the Netherlands is the acquisition and/or financing via foundations or other legal structures (charitable, religious, educational). In addition foundations can also be used by criminals to create anonymity and conceal the (beneficial) ownership of goods and properties.	ML TF
Money Service Businesses (MSB) & Payment Service Providers (PSP)	This sector has a higher risk on ML/TF due to the anonymity and less transparency. With regard to the PSP-sector, the regulation and supervision on this sector can differ per jurisdiction. To make sure that the level of regulation and supervision is adequate, an assessment similar to correspondent banking relationship needs to be performed on customers active in the PSP-sector.	ML TF