# Guidelines to the Dutch Money Laundering and Terrorist Financing (Prevention) Act (‘Wet ter voorkoming van witwassen en financieren van terrorisme, Wwft’) and the Sanctions Act of 1977 ('Sanctiewet 1977, Sanctiewet’)

Publication date: 13 October 2022. Translation of the Guidelines for the Wwft and Sanctions act of 9 October 2020

## The Dutch Authority for the Financial Markets

The AFM is committed to promoting fair and transparent financial markets.

As an independent market conduct authority, we contribute to a sustainable financial system and prosperity in the Netherlands.

## Table of contents

# 1. Introduction

These Guidelines are intended for investment firms, (managers of) alternative investment funds, (managers of) UCITS, financial service providers providing intermediary services in life insurance contracts and financial service providers that use the National Regime (and thereby qualify as investment firms), as well as branch offices in the Netherlands of institutions established outside the Netherlands. The Guidelines should be read in conjunction with the 'General Guidelines to the Dutch Money Laundering and Terrorist Financing (Prevention) Act' (Wet ter voorkoming van witwassen en financieren van terrorisme, or Wwft) issued by the Ministries of Finance and Justice and Security.

The Guidelines have been revised due to new regulations, such as the introduction of the register of Ultimate Beneficial Owners (UBO). In addition, many firms needed further explanation.

The AFM's intention with the publication of these Guidelines to offer tips and insight into the various obligations under the Wwft and the Sanctions Act of 1977 (the Sanctions Act). The Guidelines are not a legally binding document or policy rule as referred to in Section 1:3(4) of the Dutch General Administrative Law Act (Algemene wet bestuursrecht) and accordingly has and is not intended to have any legal consequence. This document should be regarded as an explanation of the Wwft and the Sanctions Act.

These Guidelines do not have the status of legislation or regulation. The approach described is not necessarily the only manner to comply with the requirements pursuant to the Wwft and the Sanctions Act. The examples presented in the Guidelines are not exhaustive, should not always be regarded as sufficient and are only intended as an illustration of a number of legal obligations. Institutions are free to comply with the requirements pursuant to the Wwft and the Sanctions Act in another manner.

## 1.1 Document structure

The Guidelines consist of two parts: part I (sections 2 to 8) deals with the Wwft and part II (section 9) deals with the Sanctions Act.

Section 2 explains the background and purpose of the Wwft, as well as the AFM's supervision in relation to the Wwft. Section 3 deals with the obligation to prepare and record an analysis of the risks associated with money laundering and the financing of terrorism and the design of policy and procedures. There is also a brief description of the obligation to design group policy and procedures for institutions that operate internationally. Section 4 lists certain obligations regarding the structure of the business operation, such as the inclusion of a compliance and audit function. Section 5 deals with a key obligation under the Wwft, namely the performance of customer due diligence, with special attention to simplified and enhanced customer due diligence. Section 6 addresses another important obligation under the Wwft, which is the obligation to report unusual transactions to FIU Nederland, with examples of situations that may lead to reports of an unusual transaction. Section 7 explains both the retention obligation and the

obligation to take (periodic) training. Section 8 lists a number of sector-specific items of attention for investment firms, (managers) of alternative investment funds, financial service providers providing intermediary services in life insurance contracts and financial service providers that make use of the National Regime (and thereby qualify as investment firms). Finally, section 9 deals with the Sanctions Act, with attention to the obligations under this Act and how institutions can meet these obligations.

The AFM also supervises compliance with the Wwft BES. The AFM has issued specific guidelines to the Wwft BES.

# Part I: The Dutch Money Laundering and Terrorist Financing (Prevention) Act

# 2. Legislation and supervision

## 2.1 Purpose and background of the Wwft

The purpose of the Wwft is to combat money laundering and the financing of terrorism. Money laundering concerns making illegally obtained money legal by concealing its illegal origins. The financing of terrorism involves the use of money to enable terrorist activities.

The Wwft came into force on 1 August 2008. The introduction of the Wwft was combined with the Provision of Services (Identification) Act (Wet identificatie bij dienstverlening, or Wid) and the Disclosure of Unusual Transactions (Financial Services) Act (Wet melding ongebruikelijke transacties, or Wet MOT). The introduction of the Wwft served to implement the European Directive on preventing the use of the financial system for money laundering or terrorist financing (the third anti-money laundering Directive).

*Fourth anti-money laundering Directive and UBO register*

The fourth anti-money laundering directive was implemented in the Wwft on 25 July 2018.

Under the (revised) fourth anti-money laundering directive, all EU Member States are obliged to maintain a UBO register. The UBO register in the Netherlands became active on 27 September 2020. Businesses are obliged to enter their ultimate owners or the persons exercising control in the UBO register. The UBO register in the Netherlands is part of the Trade Register of the Chamber of Commerce (Kamer van Koophandel, or KVK). Some of the data in the UBO register is publicly available.

*Fifth anti-money laundering Directive*

The revised fourth anti-money laundering directive (also known as the fifth) was implemented in the Wwft on 21 May 2020. The main changes to the Wwft concern virtual currency, measures in relation to high-risk third countries, anonymous prepaid cards and the exchange of information between competent authorities.

## 2.2 AFM's supervision

In the Netherlands, the AFM is the competent authority for the supervision of compliance of Wwft regulatory requirements by investment firms, (managers of) alternative investment funds, (managers of) UCITS, financial service providers providing intermediary services in life insurance contracts and financial service providers that use the National Regime (and thereby qualify as investment firms), as well as branch offices and subsidiaries in the Netherlands of institutions established outside the Netherlands. These institutions bear an independent responsibility to comply with the requirements of the Wwft.

Under Section 1d(3) Wwft, the AFM is also responsible for supervision of compliance with Regulation (EU) no. 1031/2010 of the European Commission of 12 November 2010 on the timing, administration and other aspects of auctioning of greenhouse gas emission allowances pursuant to Directive 2003/87/EC.

The AFM also supervises compliance with the Wwft BES. The AFM has issued specific guidelines to the Wwft BES. See: https://publicaties.afm.nl/handleiding-wwft-bes-en-sanctiewetgeving/handleiding-wwft-bes-en-sanctiewetgeving/.

## 2.3 Supervision of the provision of cross-border services

Foreign institutions may conduct business in the Netherlands, for instance by the provision of cross-border services or by setting up a branch office in the Netherlands. Some activities are subject to Wwft regulatory requirements.

*Incoming branch offices/service provision in the Netherlands*

Among others, the AFM supervises branch offices in the Netherlands of alternative investment funds, investment firms, UCITS and financial service providers providing intermediary services in life insurance contracts that are established outside the Netherlands.

Institutions without a branch office in the Netherlands but with a registered office in an EU Member State that provide cross-border financial or other services in the Netherlands have to comply with the anti-money laundering regulation in their country of origin. Supervision of these institutions is the responsibility of the supervisor in the relevant EU Member State.

The AFM is responsible for supervision of alternative investment funds, investment firms, UCITS and financial service providers providing intermediary services in life insurance contracts with a registered office in a third country that provide cross-border services to the Netherlands.

*Outgoing branch offices/services provided to other countries*

If an institution established in the Netherlands opens a branch office or subsidiary company in another EU Member State, the institution established in the Netherlands is expected to supervise that its branch or subsidiary complies with the anti-money laundering regulation in the recipient Member State. The AFM also supervises compliance with this obligation.

If an institution established in the Netherlands opens a branch office or subsidiary in a third country, this institution is obliged to establish whether the anti-money laundering regulation in that third country is less far-reaching than the Wwft. If this is the case, the institution must ensure that its branch or subsidiary complies with the Wwft. The AFM supervises compliance with this obligation, and therefore also on outgoing branch offices established in third countries.

# 3. Risk assessment and policy

Institutions must perform an assessment of their own risks of money laundering and terrorist financing, they must document this risk assessment and keep it up to date. When requested, this risk assessment must be provided to the AFM. In this risk assessment, the institution analyses the risks of money laundering and terrorist financing that may arise with regard to risk factors that relate to the type of customer, product, service, transaction and delivery channel and to countries or geographic areas. The institution then assesses the effectiveness of the control measures in place to counter these inherent risks, following which any gaps in the existing control measures can be identified. Based on this, the institution has to consider any additional measures to be taken. This risk assessment provides the basis for the development of the policy, procedures and measures to mitigate and effectively control the identified risks.

## 3.1 Risk assessment

Under Section 2b Wwft, an institution has to perform a risk assessment and document the results of the risk assessment and keep this risk assessment up to date. In any case, an institution must consider the risk factors referred to in annex III to the revised fourth anti-money laundering Directive in its risk assessment, which lists customer risk factors, product, service, transaction or delivery channel risk factors and geographical risk factors.

*Customer risk*

When assessing customer risk, the institution is free to make its own consideration. However, there are categories that may involve higher risk, and which may require the institution to take additional measures. This includes legal entities with complex structures, high-net worth individuals, institutions not subject to a form of supervision and customers in professions that are closely associated with money laundering and fraud. This may involve customers employed in businesses that are cash-intensive (for instance, the hospitality sector, massage salons, car dealerships, scrap dealers). Other examples are customers who execute or give instructions for transactions in unusual circumstances. This could for instance concern frequent and inexplicable switching to other institutions, or inexplicable changes of accounts in various geographic locations.

*Product, service and transaction risk*

When assessing product, service and transaction risks, the institution likewise is free to make its own consideration. When determining these risks, an institution may take note of (for instance) investments in goods that are difficult to value (art, antiques, whisky, real estate), asset management involving private banking, transactions executed in private bilateral agreements, new or innovative products or services and technologies, crypto products or products that are unusually complex. In addition, collaboration with other financial institutions based in a high-risk country can be identified as an activity with a higher risk. In cases involving a higher risk, the institution has to adapt its procedures and measures accordingly. This may involve differentiation

in terms of training. If a particular department at an institution is involved in high-risk products or services, its employees can be given additional and specific training. Risks arising from the combination of customer and product are also relevant in this context. Institutions should include the customer-product combination in its assignment of a customer to a risk category and its monitoring of the relationship.

*Delivery channel risk*

Assessment of delivery channel risk may involve the use of national or foreign intermediaries and the question of whether customer contact is in physical or solely digital form. If an institution does not physically see or speak to a customer, it will have to apply other means to obtain an adequate impression of the customer in order to properly assess any risks.

*Country risk*

An institution should perform a more in-depth customer due diligence if the country in which the customer lives or is established or has their place of business is designated as a country involving a higher risk of money laundering or terrorist financing as listed by the European Commission in Article 9 of the revised fourth anti-money laundering Directive. This list of countries designated by the European Commission as involving a higher risk of money laundering or terrorist financing is available on the European Commission website. Institutions should also consider other countries and regions that could involve higher risk. In assessing country risk, an institution is free to make its own consideration. One possible indication is if countries or geographical regions have been identified by independent sources as involving a high level of corruption or other criminal activity (such as on the basis of the Corruption Perception Index of Transparency International). In performing the assessment, an institution must in any event take account of the publications of the Financial Action Task Force (**FATF**), which identify various risk countries and risk areas that have not set up an adequate system for the prevention of money laundering and terrorist financing. These publications are available on the FATF's website and are annually revised in February, June and October (if necessary). Institutions are expected to be aware of the contents of these publications and to take appropriate measures where necessary. Countries against which the UN or the EU has imposed sanctions also qualify as high-risk countries.

*Unacceptable risk*

Institutions have to develop and document a policy on how to respond in the event that customers form an unacceptable risk. If unacceptable risks are identified, the institution may refuse to accept a customer or terminate an existing customer relationship if necessary. Institutions need to have a customer exit policy in place to ensure that they can terminate existing customer relationships in a proper manner. This policy should set out the circumstances in which an existing customer relationship has to be terminated and the procedures and time allotted for this. Some examples of unacceptable risks:

- (potential) relations appearing on sanction lists;
- shell banks (banks with no physical presence in the country in which they are located but which have a licence);
- legal entities with an opaque organisational structure (particularly if this structure is aimed at tax evasion);
- natural persons or legal entities suspected of involvement with a criminal organisation;
- customers who wish to remain anonymous or provide false identity information;
- customers who refuse to provide the legally required information documents;
- professional counterparties that do not hold the required licences, known as illegal financial firms. NB: Both the AFM and DNB have public registers listing authorised financial institutions. Here one can check whether an institution holds a licence or is registered.

*Design of the risk assessment*

The steps an institution takes to identify and assess money laundering and terrorist financing risks within its business should be appropriate to the nature and size of its business. If an institution does not offer complex products or services and has no or limited international exposure, the risk assessment need not be that complicated or sophisticated.

Managers of alternative investment funds can include the risk analysis based on the Wwft in their systematic integrity risk analysis (SIRA) that is required under Section 17 of the Market Conduct Supervision (Financial Institutions) Decree (Besluit Gedragstoezicht financiële ondernemingen, or BGfo). Investment firms and financial service providers are explicitly not obliged to conduct a SIRA under the BGfo, but they are obliged to conduct a risk assessment under the Wwft.

When performing a risk assessment, it is important that risks are not defined in overly general terms and that they are specifically related to the nature and size of the institution's business. For example, rather than describing the potential risks generally associated with politically exposed persons (PEPs), a risk assessment should address the question of whether the institution's customers include any PEPs and if so, whether these PEPs are Dutch or foreign PEPs and which specific risks this entails. Risks must then be assessed realistically by the institution and not assessed as 'low' by default without good reason.

## 3.2 Policy and procedures

Under Section 2c Wwft, an institution must have in place policies, procedures and measures to mitigate and effectively control risks of money laundering and terrorist financing that are appropriate to the nature and size of the institution's business. The institution's risk assessment must clarify the risks (under Section 2b Wwft). In addition to its own risk assessment, an institution must incorporate the supranational risk assessment (SNRA) and national risk assessment (NRA) in its policy. The supranational risk assessment is prepared by the European Commission, and lists specific, cross-border threats that could affect the internal market of the European Union. In addition, Member States conduct a national risk assessment to identify the risks of money laundering and terrorism financing. Institutions must regularly review their policy, also on the basis of updates to the risk assessments.

The policy must be detailed into clear, easily accessible procedures, including procedures for determining the risk profile of customers (such as a risk matrix for assigning customers to risk categories), continuous monitoring and audits with regard to PEPs and sanctions regulation. In addition, the policy should include a clear description and allocation of duties, powers and responsibilities within the institution.

### 3.3 Group policy and procedures

If an institution established in the Netherlands opens a branch office or subsidiary in a third country (in other words, outside Europe), this institution is obliged to establish whether the anti-money laundering regulation in that third country is less far-reaching than the Wwft. If this is the case, it must ensure that its branch or subsidiary complies with the Wwft. The institution is thus obliged to establish group policy and procedures for compliance with the Wwft that apply to the whole group, therefore also for its offices in a third country. In addition, these institutions have to ensure that their group policy and procedures are applied effectively.

# 4. Structure of business operation

An institution has to designate one of the persons responsible for determining its day-to-day policy as responsible for the institution's compliance with the Wwft. This designated day-to-day policymaker has to bear responsibility for supervising compliance with the Wwft within the institution. The institution's conduct guidance, procedures and measures have to be approved by its day-to-day policymakers. In addition, where proportionate to the nature and size of the institution's business, the institution must have in place a compliance function.

The 'nature and size' criterion concerns a combination of factors, so not only the size of the institution in terms of its number of staff members, but also its number of clients, number of foreign or high-risk clients and types of products. An investment firm with two employees and a few very high-risk foreign clients for instance would have to install a compliance function, while the same firm with a few low-risk Dutch clients would not.

The compliance function focuses on monitoring compliance with the statutory regulations and the internal regulations drawn up by the institution itself. The obvious approach is that the compliance function is responsible for testing and updating the risk assessment and the risk policy. Furthermore, the person holding the compliance function is responsible for reporting unusual transactions and providing the required information to the Dutch Financial Intelligence Unit (FIU-NL). This concerns solely the provision of the information and does not mean that the sending of a report cannot be agreed with others, such as the policymaker(s). Indeed, the qualification of a transaction as unusual will generally be the responsibility of the first-line function (the employees charged with the performance of the services provided by the institution).

In addition, if proportionate to the nature and size of the institution, an independent audit function must be put in place. For the purpose of the application of the Wwft, the audit function has to independently audit the institution's compliance with the Wwft, as well as the compliance function's performance of its duties.

Lastly, an institution has to have procedures in place to enable its employees or persons in a similar position to report a contravention of the Wwft internally. These procedures should enable reporting on an independent and anonymous basis. In addition to the above, the AFM has the option of reporting offences to the Financial Markets Hotline[1].

[1] https://www.afm.nl/nl-nl/over-afm/contact/consumenten.

# 5. Customer due diligence

This section deals with the various aspects of customer due diligence.

It begins with a general explanation of the obligation to perform customer due diligence (section 5.1). Section 5.2 discusses the identification and verification of the identity of the client or its UBOs and the documents that may be used for this purpose. The terms UBO, Pseudo-UBO and the UBO register are then explained. Section 5.3 deals with establishing and recording the purpose and nature of the business relationship. Section 5.4 describes the ongoing monitoring of the client and the transactions executed, including the monitoring of transactions, (periodic) reviews and - if necessary - establishing and recording the source of funds. Section 5.5 discusses the introduction of clients by an institution subject to the Wwft and section 5.6 deals with delegation of customer due diligence. We then turn to the option of simplified customer due diligence and the conditions that apply to this (section 5.7), including customer due diligence for listed companies. In conclusion, we explain when enhanced customer due diligence is appropriate and the requirements this form of customer due diligence has to meet (section 5.8). Particular attention is devoted here to:

- control measures for enhanced customer due diligence and some examples thereof;
- a situation in which the client is not physically present;
- the possibility of using innovative solutions and the conditions applying to this;
- high-risk countries;
- the term PEP and how enhanced customer due diligence has to be structured;
- the term ‘correspondent relation’ and how enhanced customer due diligence has to be structured.

## 5.1 Customer due diligence

Under the Wwft, an institution has to perform a customer due diligence screening before entering into a business relationship or executing a transaction. The principle here is that institutions should enter into relationships or execute transactions only with persons who do not constitute a threat to their integrity.

The Wwft has a broad definition of the term ‘customer’ (or ‘client’). In Section 1(1) Wwft, a customer is defined as a ‘natural person or legal entity with whom a business relationship is initiated or has a transaction executed’. The term ‘business relation’ is defined as a ‘business, professional, or commercial relationship between an institution and a natural person, legal entity or company that is connected to the professional activities of the institution in question and in which at the time contact is made there is the assumption that the relationship will last for some time’. This broad definition means that also relations with professional counterparties in the context of the core business of the institution fall under the Wwft, such as relationships with other institutions and service providers.

A customer due diligence screening enables an institution to:

• identify the customer;

• verify their identity;

• identify the ultimate beneficial owner and verify their identity;

• establish the purpose and intended nature of the business relationship;

• monitor the business relationship and the transactions, if necessary with review of the source of the funds used in the relationship or for the transactions;

• establish whether the natural person representing the client is authorised and to identify this person and verify their identity.

When determining the degree of customer due diligence measures that need to be applied, the institution assesses the risk of money laundering and terrorist financing. An institution has to determine how far-reaching these measures need to be on the basis of the risk sensitivity of a customer, transaction, product or service. The institution also takes account of the purpose of an account or relationship, the size of the assets deposited by a customer or the size of the executed transactions, and the regularity or duration of the business relationship.

With respect to customers that have already been accepted under the Wwft prior to the legislative change of 25 July 2018, Section 38 Wwft states that a review has to be conducted of all or parts of the customer due diligence performed in the first instance. In many cases, the first instance occurs at the time of customer contact. However, the first instance is also the time when the institution has cause to perform a customer due diligence screening on the basis of the customer's risk sensitivity. Existing customer files have to be reviewed on a risk basis, meaning that files with a high risk should be reviewed first.

## 5.2 Identification and verification of the identity of the customer and its UBOs

A customer due diligence screening consists (among other things) of identifying the customer and verifying that the identity presented corresponds to the true identity. During the screening, the institution notes whether a client is acting for their own account or for another person, in which it is important to be aware of the potential use of front men. If a client acts on behalf of another person, this other person also has to be subject to the customer due diligence screening.

Identification of the customer can be based on the details the customer provides, for instance by having them complete a (web) form. Verification of identify concerns confirmation that the identity presented corresponds to the true identity. For natural persons, the permitted means of identity verification are:

• a valid passport, identity card, or driving licence;

• a valid identity card or driving licence from an EU Member State;

• travel documents for refugees and aliens;

• alien's identity card.

It cannot be assumed in advance that adequate identification and verification has been carried out for documents not originating from a government institution or a court, such as student identity cards, employee cards or bills from utility or telecom companies. In general, such documents are not sufficient for verification of identity.

The Guidelines 'Identification and verification of personal data' from the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) state that a financial institution - as evidence that it has fulfilled its obligation to identify (obligation to reconstruct) may archive a copy of the identity document reviewed. However, this is not mandatory: recording (or copying) certain details appearing in the document is sufficient. There is no obligation to record the Citizen Service Number (BSN) under Section 33 Wwft.

*Ultimate Beneficial Owners (UBOs)*

The identification of a UBO plays a role if the customer of the institution is a legal entity. It must be clear which natural person is - ultimately - behind the legal entity. The institution must take adequate measures to ensure that the stated identity of the UBO corresponds with the actual identity as well as what the nature and size is of the ultimate interest held. For corporate structures, the principle is that the institution should know and understand the customer's ownership and control structure. This means, for example, that in the event of a complicated structure consisting of many companies, the institution must make more of an effort to understand the (international) structure of the customer than for a Dutch private company with a director-major shareholder.

The definition of an ultimate beneficial owner is given in Section 1 Wwft. The two criteria that are of importance to qualify a person as a UBO concern the possession of ultimate ownership or having ultimate control of a customer via the holding of shares, voting rights, ownership interest or other means. Section 3 of the Wwft Implementation Decree 2018 (Uitvoeringsbesluit Wwft 2018) gives further details of persons qualifying as UBOs.

- For Dutch public or private limited companies (a B.V. or an N.V.), this is the natural person directly or indirectly entitled to more than 25% of the financial value of the company, or the person exercising control. This 25% rule does not apply to listed companies; see the following paragraph for more information on UBOs of listed companies;
- For foundations and associations, the UBO is the natural person directly or indirectly owning more than 25% of the company, or the person able to cast more than 25% of the votes in the event of an amendment to the articles of association, or the person exercising de facto control of the legal entity;
- For a general partnership (*VOF*), professional partnership (*maatschap*), limited partnership (*CV*) and shipping companies, the UBO is the natural person directly or indirectly owning more than 25%, or the person able to cast more than 25% of the votes with respect to management acts and/or amendments to the partnership agreement;
- For a church, the UBOs are the natural persons named as legal beneficiaries in the church's constitution.

In the case of a trust, there must be more than one person named as the ultimate beneficial owner. These are in any case the trustees of the trust, but also the founder, the protector if applicable and the beneficiaries of the trust.

Natural persons holding smaller interests may also be designated as ultimate beneficial owners, for instance because they are able to exercise ultimate control of a customer in other ways. From the definition of an ultimate beneficial owner, it follows that not only natural persons holding ultimate ownership or ultimate control of a legal entity or company should be designated as ultimate beneficial owners. A natural person should also be designated as an ultimate beneficial owner if the ultimate ownership or ultimate control is held indirectly, for example through another legal entity or legal construction, such as a trust or mutual fund.

*UBOs of listed companies*

The 25% rule for public and private limited companies (a B.V. or an N.V.) stated above does not apply to listed companies that are subject to disclosure requirements that ensure adequate transparency of ownership information. These are the disclosure requirements as stated in the Transparency Directive or comparable international standards. Since listed companies are already subject to disclosure requirements, and have therefore published information on their ownership and UBOs, it is not considered necessary in such cases to again designate the relevant natural persons as ultimate beneficial owners. The Wwft and supporting regulation therefore do not list any categories of natural persons who in any case have to be designated (in advance) as UBOs of listed companies that are subject to disclosure requirements. In other words, no alternative objective measure (such as the 25% rule) is given.

It may however be the case that a listed company has a UBO. One indication of this is the percentage of share capital that is freely marketable. An institution thus has to assess whether a customer that is a listed company has a UBO. It is therefore for the institution to assess on the basis of certain criteria and information whether it designates a person as a UBO of a listed company that is subject to disclosure requirements. This can be assessed on the basis of annual reports or other public sources of information. The institution's assessment should be recorded and substantiated, for example in its Wwft policy.

For the question of whether, and if so how, the UBO(s) of a listed company should be investigated, see the section on 'simplified customer due diligence'.

*UBO register*

From 27 September 2020, companies are obliged to enter their ultimate owners or the persons exercising control in a UBO register. This register, in which information on UBOs is recorded, will be part of the Trade Register and thus be managed by the Chamber of Commerce. Some of the information on UBOs will be publicly available.

The obligation to register a UBO applies to the following organisations:

- (non-listed) Dutch private and public limited companies (*besloten vennootschappen* (BVs) and *naamloze vennootschappen* (NVs));
- other legal entities: foundations, associations with a UBO, mutual insurance associations and cooperatives;
- partnerships: professional partnerships (*maatschappen*), general partnerships (*vennootschappen onder firma*), and limited partnerships (*commanditaire vennootschappen*);
- shipping companies;
- European public limited companies (Societates Europaea, or SEs);
- European cooperative societies (SCEs);
- European economic interest groupings (EEIGs);
- churches.

A feedback obligation has been introduced for institutions subject to the Wwft. This means that institutions subject to the Wwft are obliged to inform the Chamber of Commerce if they establish that the registered details of their UBO or pseudo-UBO are incorrect or incomplete (discrepancies). This obligation does not apply if notification is made to the FIU-Nederland.

No feedback has to be given for a registration not yet made during what is known as the 'completion period' of 18 months following the introduction of the UBO register on 27 September 2020. The opposite applies if details have already been registered: in this case, the feedback obligation also applies during this 18-month period.

When entering into a new business relationship with a client, an institution must establish whether the client's UBO is entered in the UBO register. The institution must also ensure that proof of inclusion in the UBO register is included in the client's file. This is in addition to the institution's own obligation to identify the UBO and verify the UBO's identity. When performing a customer due diligence, institutions may not rely solely on the information in the UBO register. This means that an institution must itself also establish the identity of the UBO.

*Pseudo-UBOs*

In certain specific cases, all persons part of the senior management (such as directors or partners) are registered as pseudo-UBOs. For example, if no UBO can be found on the basis of shareholdings, voting rights or ownership. This regulation ensures that an ultimate beneficial owner can be registered for every legal entity. The designation of senior management personnel as pseudo-UBOs is a last resort and is acceptable only after all possible means of identifying the UBO have been exhausted and provided that there are no grounds for suspicion, or if there is any doubt as to whether the UBO is indeed the ultimate owner or exercises control.

In this regard, 'senior management personnel' should be understood to include all the customer's directors under the articles of association or, as applicable, all partners in a partnership. This also applies to non-executive directors in a one-tier board.

*Reasonable measures*

'Reasonable measures' means that an institution must make a reasonable effort in its customer due diligence to verify the identity of a UBO. Verification of identity, however, takes place continuously. The intensity of verification may be adjusted according to the risk associated with the client or transaction. This means, for example, that in the event of the involvement of a higher risk, the institution must base the verification of the identity of the UBO on documents and information from a reliable and independent source. A copy of proof of identity for example is not information from a reliable and independent source. To verify the identity of a UBO, an institution may not solely rely on information on the UBO provided by the client (the so-called UBO declaration (UBO-verklaring)). An institution can also use various public sources and registers such as the Trade Register of the Chamber of Commerce in addition to an identity document to verify the identity of a UBO.

If an institution is unable to establish the identity of a UBO or designate a pseudo-UBO, for example due to suspicions, it may not enter into a business relationship with the client and/or may not execute the requested transaction.

## 5.3 Purpose and nature of the business relationship

Obtaining information on the purpose and nature of the business relationship enables an institution to assess the risks of providing services to the client in question. Some of this information will usually be obtained during contact prior to entering into the business relationship. The products or services to be purchased may be an indication of the purpose and envisaged nature of the business relationship. For example, this could be demonstrated by the record of an agreement in the client's file. If the client is not resident or established in the Netherlands, the institution will have to ask additional questions to determine why the client wishes to purchase products or services from the institution in the Netherlands.

## 5.4 Continuous monitoring

Under Section 3(2(d) Wwft, an institution must continuously monitor a business relationship and the transactions executed during this relationship. This is done by formulating a risk profile for the client based on the customer due diligence screening, monitoring of transactions and periodic reviews, if necessary with a review of the source of funds used in the business relationship or transaction. The institution has to ask questions in this regard and record explanations and supporting documentation in the client's file. The institution has to establish indicators in advance for determining the depth of its screening. Especially for higher-risk situations, it is sensible to establish and record the source of funds by means of independent and reliable sources.

*Transaction monitoring*

Continuous monitoring of a business relationship and the transactions executed during the relationship is mandatory under Section 3(2)(d) Wwft. This is necessary to assess whether the transactions correspond to the information the institution has on the client and the client's risk profile.

An institution has to formulate a risk profile during the customer acceptance procedure. An expected transaction pattern should also be formulated, showing the client's proposed individual transaction behaviour. The transaction profile and risk profile should both be used in the monitoring of transactions.

Monitoring (whether automated or manual) can be carried out using specific detection parameters, with associated threshold amounts. It is important that the detection parameters and threshold amounts correspond to the type of transaction and client.

Any deviant transaction patterns can also be reason for the institution to report an unusual transaction to the FIU. Since money laundering and terrorist financing are a serious threat to the integrity of an institution's business operation, an unusual transaction frequently qualifies as an incident. It is the institution's responsibility to assess whether an unusual transaction also qualifies as an incident. Any incident must be instantly reported by the institution to the AFM.

*Periodic reviews and event-driven reviews*

An institution must periodically update its information on a client and, if necessary, update the client's risk profile. Its policy and procedures should describe the manner and frequency of this update process. There is thus a clear cycle for each risk category or client type. For example, this could for high-risk clients be at least once a year, for medium-risk clients once every two years, and for low-risk clients within five years or on the basis of a clearly described event-driven review, in other words a review prompted by a particular event or trigger. The policy will also state the events prompting a client review.

One element of regular reviewing may be that the institution monitors external signals regarding a client, such as bad publicity. This can be done by means of an external system or independently, for instance by running checks on the client's name in conjunction with other search terms such as 'fraud', 'corruption', 'terrorism' and 'money laundering'.

The periodic review of clients and the monitoring of transactions are complementary processes; a periodic review will also consider transaction history.

*Source of funds*

When entering into and monitoring a business relationship, the principle is that, if necessary, the institution knows the source of the funds used in the business relationship or transaction. The institution has to ask questions in this regard and record explanations and supporting documentation in the client's file. The institution has to establish indicators in advance for determining the depth of its review of the source of funds. Especially for high-risk situations, it is sensible to establish and record the plausibility of the source of funds by means of documents, data or information from a reliable and independent source. The fact that the funds originate from an account at a Dutch bank that is also subject to Wwft supervision does not necessarily mean that the institution does not have to investigate the source of funds used in the business relationship or transaction.

If a client fails to cooperate with a review into the source of funds, the institution may not execute any transactions for that client and must terminate or refuse to enter into a business relationship.

## 5.5 Introduction of clients by an institution subject to the Wwft

An institution may adopt the information (other than the information obtained in accordance with Section 3(2)(d) Wwft from continuous monitoring) from a customer due diligence screening previously conducted if this screening has been performed by:

- a lawyer or (junior) civil-law notary in the EU, or similar legal professional;
- a registered accountant, accounting consultant with certification authority or tax consultant in the EU;
- a trust office in the Netherlands;
- regulated banks and other institutions in the EU.

According to the legislature, this is permitted because these entities are also institutions as defined in the Wwft or subject to similar supervision in another Member State. The principle, however, is that the institution remains responsible for the customer due diligence screening and the client risk assessment and must have all the identification, verification and other data relating to the identity of the client, the UBO and the representative in its possession. The AFM accordingly recommends that an institution establishes that the introducing institution has adequate Wwft procedures and measures in place and that these are complied with, especially in a situation in which an institution regularly introduces clients. An institution obtaining a client through an introduction can request the introducing institution to provide details of its Wwft procedures and assess and test on a random basis whether its customer due diligence screenings have been performed correctly. Nonetheless, an institution using information from a third party remains responsible for the continuous monitoring of its clients and must carry out its own client risk assessments. This responsibility also includes the provisions relating to the retention of documentary evidence.

## 5.6 Delegation of customer due diligence to third parties

The legislature has drafted a separate section dealing with delegation of customer due diligence to ‘a third party’ (thus not an institution subject to the Wwft): Section 10 Wwft.

When delegating customer due diligence to a third party, an institution must adequately substantiate why it relies on a customer due diligence performed by the third party in question. Similarly to introduction by an institution subject to the Wwft, here too the institution remains responsible for the customer due diligence screening and the client risk assessment. If and to the extent that this delegation occurs on a regular basis, a written agreement covering the provision of this service is mandatory. The institution instructing the third party is obliged to establish this in writing.

But please note, continuous client monitoring, including the monitoring of transactions, may not be delegated to a third party. Continuous client monitoring may however be ‘delegated’ within an

institution's group. This cannot be qualified as 'delegation' as referred to in Section 10 Wwft, as this does not involve having activities performed by a 'third party'. This is considered to be allocation of duties within a company's group.

## 5.7 Simplified customer due diligence

Simplified customer due diligence by an institution is sufficient for clients that by nature entail a low risk of money laundering or terrorist financing. Simplified customer due diligence means that the institution demonstrably obtains and updates information substantiating that simplified customer due diligence is adequate. The customer due diligence screening must be carried out in any event, but the depth of the customer due diligence measures applied may be adjusted according to the risk associated with the type of customer, product, service, transaction and delivery channel or with countries or geographic areas.

Contrary to what was previously the case, the current version of the Wwft does not designate any types of customers for which simplified customer due diligence is considered to be adequate. An institution should always conduct a prior risk assessment on a case-by-case basis before entering into a business relationship or executing a transaction to assess whether this represents a low risk. If there is proven low risk, simplified customer due diligence measures will suffice. An institution may in any case take account of the non-exhaustive list of low risk factors in Annex II of the revised fourth anti-money laundering directive. For example, this annex mentions listed companies, public administrations or enterprises or life insurance policies for which the premium is low.

*Listed companies*

Formerly, the Wwft stated that customer due diligence was not necessary if the client was a listed company However, since the revised fourth anti-money laundering directive came into effect, this is only a low risk factor. There is thus no longer any exclusion of the obligation to perform a customer due diligence screening with respect to listed companies and their UBOs. Being a listed company subject to certain disclosure requirements is stated as a low risk factor in Annex II of the revised fourth anti-money laundering directive. It is important that institutions do not automatically assume that listed companies by definition entail a lower degree of risk. Indeed, risk factors that are not client-specific may apply with respect to the type of product, service or transaction as well as geographical risk factors. Factors such as the exchange on which the company is listed, where the company or exchange is located or the percentage of freely marketable share capital may for instance be relevant. This means in any case that for more complex clients, a simplified customer due diligence screening will not automatically be sufficient for a listed company. There will always have to be a risk analysis based on more than a market listing, and the institution will have to demonstrate that a simplified customer due diligence is sufficient.

The institution has to determine whether the client is subject to the disclosure requirements referred to in the Transparency Directive or equivalent requirements. There is no officially

recognised list of countries or listed companies that apply equivalent disclosure requirements. The institution accordingly has to carry out an assessment to determine whether this is the case.

Listed companies may have non-tradable shares as well as tradable shares. If these unlisted shares are not subject to disclosure requirements, the requirements for making an exception are not met and the institution will have to perform a regular customer due diligence screening. Non-tradable share capital is thus not covered by a simplified customer due diligence screening. An institution subject to the Wwft will therefore have to establish the extent to which its client is a listed company.

Briefly, the following applies. If a client subject to the Wwft:

i) is a publicly listed company;

ii) that is subject to certain disclosure requirements, and

iii) the disclosure requirements apply to the entire share capital, and

iv) there are no other high-risk factors that require a regular customer due diligence screening,

a simplified customer due diligence screening on the basis of Section 6 Wwft and the institution subject to the Wwft does not have to identify a UBO or pseudo UBO or verify this identity.

This does not change the fact that the identity of major shareholders or senior management may be important for the purpose of the Wwft as part of the review of the client's ownership and control structure and the ability to screen relations against sanctions lists. It is therefore important that institutions subject to the Wwft take note of the information made available due to the disclosure requirements and that they record this information.

*Timing of identification*

Section 4(1) Wwft states that an institution should verify the identity of the client or UBO prior to entering into a business relationship or transaction. In derogation to this, the third paragraph states that an institution may complete its verification of the identity of the client or UBO during the process of entering into the business relationship to avoid unnecessary disruption to the normal provision of services. This is however subject to the condition that this is only permitted in situations in which it is necessary to avoid disruption to the provision of services, the risk of money laundering or terrorist financing is low and that identification is completed as soon as possible after the initial contact. Under Section 4(4) Wwft, it is permitted to open an account, including a securities trading account, before identification of the client's identity has taken place if the institution ensures that this account cannot be used before verification has taken place. This can for example be by blocking the account until the client's identity has been verified.

## 5.8 Enhanced customer due diligence

In cases involving a higher risk of money laundering or terrorist financing, an institution must perform an enhanced customer due diligence screening. In these cases, and also in cases qualified

as high risk under the previous legislation, an institution must carry out enhanced measures. An enhanced customer due diligence screening must be performed if a business relationship or transaction by its nature represents a higher risk. The institution must establish whether a higher risk is present on the basis of a risk assessment prior to entering into a business relationship or executing a transaction. In this risk assessment, an institution must in any case take account of the risk factor stated in Annex III to the revised fourth anti-money laundering directive. Institutions must also investigate all complex and unusually large transactions and all unusual transaction patterns that do not have an apparent economic or legitimate purpose. In such cases, the institution will subject the entire business relationship with the client to enhanced monitoring.

Like its fellow supervisors around the world, the AFM has previously warned of the risks associated with cryptos. Since transactions with cryptos by their nature involve a higher risk of money laundering or terrorist financing, an institution must always perform an enhanced customer due diligence screening. Among other things, this means that institutions perform an enhanced customer due diligence screening on clients participating in the collective investment scheme, clients that are professional counterparties and correspondent relations. Other potential risks concern a client's involvement in high-risk activities or sectors, such as cash-intensive activities or the real estate sector.

*Control measures*

In cases involving higher risk, an institution will take enhanced measures and will have to obtain and check more information on the client to mitigate and manage this higher risk. The measures taken in an enhanced customer due diligence screening include:

- obtaining a larger quantity of information used for customer due diligence (CDD) purposes, such as:
    - information on family members and close business partners;
    - information on previous and current business activities and sources of income of the client or UBO; and
    - (in-depth) searches for unfavourable publicity in the media.
- validation of information obtained from independent and reliable sources obtained for CDD purposes to confirm the identity of the client or UBO, including establishing that the assets and funds of the client to be used in the business relationship do not originate from criminal activity. The source of funds or assets may be verified by reviewing value-added tax or income tax returns, copies of accounts audited by an external auditor, salary statements, public acts or articles in independent media.
- increased frequency of periodic evaluations and more in-depth transaction monitoring.

*Client is not physically present*

The requirement in Section 8(2) of the former Wwft, that an institution must perform an enhanced customer due diligence screening if a client is not present for the verification of their

identity, has lapsed. The measures to compensate for higher risk have also lapsed, such as the name-number check (known as the '1 cent transfer').

However, Annex III to the revised Fourth Anti-Money Laundering Directive qualifies 'non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures' as involving higher risk. An institution should in any case take account of this risk factor in its risk assessment. If a client is not physically present, institutions can verify their identity remotely using innovative technologies. They must at least take account of the following risk factor Annex III to the revised Fourth Anti-Money Laundering Directive: '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.'

*Innovative solutions*

Institutions are free to devise innovative solutions for verifying identity. These include verification of a client's identity (if not present in person) on the basis of traditional identity documents (such as a passport, driving licence or national identity card) by means of various portable devices such as a smart phone.

Institutions using innovative CDD solutions need to include other risk factors in their risk analysis as well as the usual risk factors (client, product, services, transaction, delivery channel and geographical risk factors). The institution needs to assess whether:

- it has the necessary technical skills to oversee the development and correct application of innovative solutions, especially if these solutions are developed or used by a third party;
- the senior management and the compliance officer have sufficient knowledge of the innovative solution to be used; and
- institutions have an emergency plan to safeguard the continuity of the CDD. The continuation of the services needs to be safeguarded in the event that the innovative solution is subject to (irreparable) system breakdowns, or if a business relationship between the institution and an external supplier of the solution is terminated (if the solution has not been developed internally).

The risk factors listed above are developed and further specified 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'.

*High-risk countries*

Furthermore, an enhanced customer due diligence screening needs to be performed if the client or the client's UBO is resident or located, or has its registered office, in a country designated by the European Commission as a high-risk country. These are third countries whose national legislation to prevent money laundering and terrorist financing contains strategic shortcomings that form a material threat to the European Union's financial system.

In addition, an institution will have to carry out the following enhanced investigative measures with reference to transactions, business relationships and correspondent banking relations related to countries designated by the European Commission as countries with a higher risk of money laundering or terrorist financing:

- obtaining additional information on these clients and their ultimate beneficial owners;
- obtaining additional information on the purpose and nature of the business relationship;
- obtaining information on the source of the funds to be used in the business relationship or transaction and the source of the assets of these clients and their ultimate beneficial owners;
- obtaining information on the background of and motivation for the proposed or executed transactions of these clients;
- obtaining approval from senior management for entering into or continuing the business relationship;
- employing enhanced monitoring of the business relationship with and the transactions of these clients, by increasing the number of checks and the frequency of updates of data on these clients and ultimate beneficial owners and selecting transaction patterns that require further review.

This also means that if a Dutch legal entity has a UBO from one of these countries or if there are money transfers from or to one of these countries, the institution must apply these enhanced customer due diligence measures.

*PEPs*

PEP stands for 'politically exposed person' (in Dutch, 'politiek prominent persoon'. A PEP is a person holding a prominent political office and their direct family members (partners, adult or minor children and parents) or close associates (for example, persons with a close business relationship to the PEP) of these persons. The term PEP is no longer limited to non-Dutch politically exposed persons: it now covers national politically exposed persons as well.

PEPs in any case include:

a. heads of state, heads of government, ministers, junior ministers or state secretaries;
b. members of parliament or similar legislative body;
c. members of the administration of a political party;
d. members of a high court, constitutional court or other high judicial authority making rulings that are not open to appeal, except in exceptional circumstances;
e. members of an audit office or executive board of a central bank;
f. ambassadors, chargés d'affaires or senior officers of the armed forces;
g. members of the management body, supervisory body or governing body of a state enterprise;
h. directors, deputy directors, members of the management board or holders of similar functions at an international organisation.

Mid-level or junior officers are not politically exposed persons.

Business relations with PEPs require additional measures, as this group involves an increased risk of reputational damage, corruption and other risks. An institution must have risk-based procedures in place in order to determine whether a client or its UBO is a PEP. There are various ways for institutions to establish whether they are dealing with a PEP and the status of the PEP concerned. Firstly, the institution can make use of the information obtained from the customer due diligence screening. It can however also use the services of commercial businesses that publish lists of PEPs for a fee. An institution can also consult public sources. Simply requesting current or future clients or UBOs to state whether they are a PEP is not sufficient to qualify as a risk-based procedure. An institution may not rely solely on what a client says, it must conduct its own review.

Enhanced customer due diligence measures are required in all cases involving transactions or business relationships with clients that qualify as PEPs or their UBO qualifies as a PEP, or in cases where the beneficiary of a life insurance or the UBO of that beneficiary is a PEP. Firstly, this concerns suitable measures to establish the source of the assets and funds to be used in the business relationship or transaction. Approval must also be obtained from a member of the senior management before entering into or continuing the business relationship or executing the transaction. The senior management of the institution concerns the day-to-day policymakers, and managers directly below the level of the day-to-day policymakers who are authorised to make decisions regarding the institution's exposure to certain risks, including the risks of money laundering and terrorist financing. The business relationship is subsequently subjected to enhanced checks and transaction monitoring.

For the review of the source of assets and funds to be used in the business relationship, an institution will initially contact the client so that the client is made aware of its status as a PEP. The institution will at this point request the client to provide information on the source of its assets. The client is expected to provide information that is sufficient for the institution to no longer have questions regarding the source of the assets.

In this review, particular attention will be devoted to circumstances that differ from what might be reasonably expected for the specific client in question. In many cases, information on employment, as shown for example in tax returns, will suffice. This information can be requested from current or former employers, if necessary. In cases where a PEP's assets originate from another source, additional information will be needed.

The point here is that an institution is ultimately able to establish that what it knows about the source of the PEP's assets corresponds with what it knows about its client and the purpose and nature of the proposed business relationship. This way, an institution can ensure that its services will not be used for money laundering.

The risk-based approach required under the Wwft for the performance of customer due diligence screenings requires specific work. This also applies in cases involving an enhanced customer due diligence screening of a politically exposed person. For example, the level of risk associated with the parents of a Member of the House of Representatives who hold an ordinary bank account will

thus be lower than the risk related to the daughter of a head of state of a country with an increased risks of corruption who is investing in private equity or high-risk assets. The degree of intensity of the measures should correspond to the specific risks in the case concerned. For example, this could be realized by consulting multiple sources for verification of the information obtained with regard to the assets of a PEP. If the level of risk is assessed as low, in some cases this information may be verified on the basis of a public source, such as the internet.

The risk associated with a specific case will also determine the frequency of checks by the institution that the information obtained from its customer due diligence screening is still up to date. A client may, after all, become a PEP as a result of appointment to another function or position. Information has to be updated on a periodically. Institutions may also take note of signals that could lead to a change to the client's risk profile. If there are no such signals, and the risk is assessed by an institution as low, it may be that some considerable time has passed between the time the initial customer due diligence screening was performed and the next time the institution contacts the client. It is indeed not necessary in all cases to contact clients to assess whether previous information is still up to date.

If a client or its UBO no longer holds a politically exposed function, the enhanced measures must in any case continue to be applied for one year and also subsequently, until such time as the person concerned no longer represents a higher risk.

*Correspondent relations*

The obligation to perform an enhanced customer due diligence screening for 'correspondent relations' also applies to institutions other than banks, and includes alternative investment funds, investment firms and financial service providers providing intermediary services in life insurance contracts.

Correspondent relations concern relationships between institutions initiated for services such as cash management, money transfers, transit accounts, currency exchange services and securities transactions.

If such a relationship is entered into with a party not located in the EU, sufficient information must be obtained on this other institution to establish a full understanding of the nature of its business activities. The reputation of this institution must be assessed on the basis of publicly available information and the quality of the supervision to which it is subject. The other institution's procedures and measures to prevent money laundering and terrorist financing must also be assessed and the responsibilities of both institutions must be recorded.

In cases involving a new correspondent relationship, the decision to enter into the relationship must be taken or approved by senior management. This enhanced customer due diligence screening can be performed on a risk basis, meaning that the intensity of the measures can be set according to the risk represented by the correspondent relation.

# 6. Reporting unusual transactions

Under Section 16 Wwft, an institution is obliged to report an executed or proposed unusual transaction to FIU Nederland. The Wwft defines a transaction as an action or combination of actions by or on behalf of a client that the institution has become aware of in the performance of its service to the client in question. It is not a requirement that there is a direct or causal relationship between the unusual transaction and the activities of the institution. The timing of an unusual transaction is, in principle, irrelevant for the purpose of this reporting obligation.

## 6.1 Objective and subjective indicators

The Annex to Section 4 of the Wwft (Implementation Decree) 2018 lists objective and subjective indicators per type of institution on the basis of which an assessment has to be made as to whether a transaction can or has to be designated as unusual.

For (managers of) alternative investment funds, UCITS, investment firms and financial service providers providing intermediary services in life insurance contracts, only the so-called subjective indicator applies, namely: 'transactions giving the institution reason to believe that the transaction could be linked to money laundering or terrorist financing'. The subjective indicator entails an obligation to report on the basis of the assessment the institution has itself made; in this case, the Wwft relies on the professional opinion of the institution concerned to determine whether a particular transaction is unusual. According to the subjective indicator, the institution has to report a transaction that it has reason to believe could be linked to money laundering or terrorist financing.

Examples of circumstances that could indicate that a transaction is unusual:

- lack of clarity regarding the underlying parties or ultimate beneficiaries, for instance by the use of front men;
- pretence of a legal source of funds by wrongfully describing these as consultancy fees, commissions, or loans;
- unusual sources of funds, for instance from countries featuring a high level of corruption and political instability, or the involvement of offshore companies;
- funds originating from foreign accounts held by Dutch citizens opened with the aim of keeping these funds out of sight of the Dutch authorities;
- unusual and unaccounted for income, such as a false inheritance, lottery winnings or failure to cite sources other than non-verifiable sources to account for the funds;
- absence of accountability documentation, such as invoices, bank statements, purchase contracts or loan agreements;
- refusal by the client to account for the source of the funds;
- transactions or investments that by nature or volume are unusual for the client in question;
- the client is an unregulated nominee company with unknown shareholders;
- the client resides or is located in a jurisdiction with a higher risk of money laundering and terrorism financing or high-risk countries, such as tax havens, countries with banking secrecy,

countries in which many offshore companies are established or countries producing illegal drugs;
- the client is also a financial enterprise, but is not registered or is registered in a jurisdiction with weak AML/CFT supervision;
- the client is involved in or derives their assets or income from potentially high-risk activities or sectors, such as cash-intensive activities, the real estate sector, the trust sector, money transfers or offshore companies;
- the client is a legal entity with 'floating assets', such as a Trust, a *Stiftung* (German foundation), a *Treuhand* (Swiss trust) or an *Anstalt* (an 'Establishment' in Liechtenstein).
- The client uses products or services that could lead to anonymity or lack of clear information on underlying customer transactions (such as bearer shares or omnibus accounts).

A report also has to be made in cases where the customer due diligence has not produced the information required by law, and there are also 'indications' that the client in question is involved in money laundering or terrorist financing. In addition, a report has to be made in the event that an existing client relationship is terminated because not all the information prescribed by law has been received and there are 'indications'. In these situations, the report must also state why the customer due diligence screening has not been successful (Section 16(4) Wwft).

### 6.2 Reports to FIU

Before an institution can make a report, it has to be registered with the FIU. The reporting procedure is explained on the FIU website under 'Reporting'. It is important that institutions report using the correct reporting group: if, for instance, an institution has both a banking licence and a licence to operate an investment firm and the unusual transaction has occurred in connection with the investment firm, the report should be made using the investment firm group.

If an institution concludes that a transaction is unusual, the transaction must be reported to the FIU. A report of an executed or proposed unusual transaction has to be made without delay, as soon as the unusual nature of the transaction becomes apparent (Section 16(1) Wwft). The details of what the report should include are stated in Section 16(2) Wwft. These include the client's identity, the identity of the UBO and - as far as possible - the identity of the party on whose behalf the transaction is effected. The report must also clearly state the circumstances leading to the transaction being qualified as unusual. Failure to report an unusual transaction when the institution is aware of its unusual nature is an economic offence under Section 1(2) of the Economic Offences Act (Wet op de economische delicten, or WED).

### 6.3 Indemnification

The Wwft includes a criminal and civil-law indemnification for institutions making a report to the FIU. The criminal indemnification is stated in Section 19 Wwft. This means that the information provided by an institution in connection with its report cannot be used for investigative proceedings or a criminal investigation of the institution relating to money laundering and terrorist financing. Qualification for a criminal indemnification with respect to a reported

transaction is explicitly subject to the condition that the report is made in good faith. In other words, that the institution has not intentionally cooperated with the facts in question. The civil law indemnification is stated in Section 20 Wwft. This means that an institution cannot be liable under civil law for losses suffered by another party as a result of the report. This civil law indemnification is subject to the condition that the institution has acted in the reasonable assumption that it has met its obligations under Sections 16 and 17 Wwft.

### 6.4 Confidentiality

Sections 22 and 23 Wwft contain an obligation to observe confidentiality with respect to reports that have been made. An institution that has reported or provided further information is obliged to keep the report confidential. Under Section 23a Wwft, an institution may share information relating to a report made in accordance with Section 16 Wwft by that institution within its group, unless the FIU instructs otherwise.

As the supervisory authority, the AFM may request institutions to provide their reports to the FIU and does so on a regular basis. The AFM checks that the institution's report to the FIU was made on a timely basis and assesses the quality of these reports. The AFM distils these reports using case-based reasoning and publishes them - in anonymous form - on its website. This case-based reasoning is regularly supplemented. See https://www.afm.nl/nl-nl/professionals/onderwerpen/wwft-voorbeelden-ongebruikelijke-transactions.

### 6.5 Incident reporting

Money laundering and terrorist financing are a serious threat to the integrity of an institution's business operation. An unusual transaction that has been executed may therefore qualify as an 'incident' as defined in Section 1 of the Market Conduct Supervision (Financial Institutions) Decree (Besluit Gedragstoezicht financiële ondernemingen, or BGfo). The institution assesses whether an unusual transaction also qualifies as an incident. Managers of alternative investment funds, to the extent that they offer participating units to retail investors, UCITS, investment firms and financial service providers are obliged to report incidents to the AFM without delay.

### 6.6 Follow-up

Finally, it may be the case that the report to the FIU leads to additional measures being taken with respect to the client in question. These may include increasing the client's risk profile or increasing the frequency of monitoring the client's transactions.

# 7. Recording, retention obligation and training

## 7.1 Recording and retention obligation

Section 33 Wwft states that an institution that has performed customer due diligence screenings on the basis of the Wwft must record the documents and information that were used for compliance with the provision of Section 3(2) to (4), Section 3a(1), Section 6(1) and (2), Section 7(2) and Section 8(3) to (6) and (8) Wwft in a retrievable manner. Among other things, this means that the data recorded for legal entities also includes the data on the persons acting for the legal entity at the institution. For the UBO, the identity of the UBO and how this has been verified is also recorded. The file will also state how the decision-making process for acceptance of the client proceeded, for instance if it concerns high-risk clients. The various files must be easily accessible for the supervisor.

An institution has to record, archive and retain data on unusual transactions for five years so that a transaction can be reconstructed (Section 34 Wwft). The recording and retention of personal data obtained in connection with the Wwft (for instance, for the customer due diligence) is processing of personal data as defined in the GDPR.

*General Data Protection Regulation (GDPR).*

The current Wwft takes account of the GDPR. Purpose limitation is an important principle in the GDPR. This principle states that personal data may only be processed for specified, explicitly described and legitimate purposes. Further processing of personal data for purposes incompatible with these purposes is not permitted. This principle is explained further in Section 34a Wwft. This states that under the Wwft, institutions subject to the Wwft may only process data for the purpose of preventing money laundering and terrorist financing (the purpose). Personal data may not be further processed in a manner not compatible with this purpose. Further information on this issue is provided in the 'General Guidelines to the Dutch Money Laundering and Terrorist Financing (Prevention) Act' issued by the Ministries of Finance and Justice and Security.

## 7.2 Training

An institution must ensure that its employees and day-to-day policymakers are familiar with the provisions of the Wwft. They should be trained to recognise unusual transactions and know how to perform a proper and full customer due diligence screening. Training needs to be provided on a regular basis, instead of solely on one occasion, so that developments are followed and awareness is maintained.

For training to be as effective as possible, it is important to structure it appropriately for the various functions at the institution. The content, depth and frequency will thus relate to the work of the employee in question. It is sensible for the compliance function to attend additional training so as to remain up to date with developments in legislation and regulation and the risks of money laundering and terrorist financing. The day-to-day policymakers – who bear

responsibility for compliance with the Wwft and the Sanctions Act – should receive training that enables them to fulfil this (ultimate) responsibility.

The structure of the training to be provided is for the institution to decide. Options include certified training courses, internal or external courses, e-learning modules and awareness sessions. Institutions do need to be able to substantiate (with material) how the courses they provide meet the training requirement in the Wwft. For instance, an undocumented weekly discussion of Wwft issues at team meetings does not quality as training. Adequate recording of the training offered, the courses taken, the frequency and the people who take the courses will enable institutions to continually establish, monitor and respond to the level of knowledge in the organisation.

# 8. Sector-specific focus items

This section deals with the AML/CFT risks that may arise in the various types of service provision by investment firms, (managers of) alternative investment funds, financial service providers providing intermediary services in life insurance contracts and financial service providers that are subject to the National Regime.

National and international sources exist that can assist institutions in their compliance with anti-money laundering regulation. Some of these are listed below:

The ESAs (EBA, ESMA and EIOPA) published joint guidelines on certain risk factors on 4 January 2018. These contain sections that relate to investment firms (sections 5 and 8), collective investment schemes (section 9) and financial service providers providing intermediary services in life insurance contracts (a subsection of section 7). They also list general instructions on how financial institutions can structure their risk assessment process (section 2).

The FATF published its 'Risk-Based Approach Guidance for the Securities Sector' and 'Risk Based approach for the Life Insurance Sector' on 25 October 2018. This guidance offers specific advice and examples for investment firms, managers of alternative investment funds and financial service providers providing intermediary services in life insurance contracts on a risk-based approach to compliance with the Wwft.

One important item of attention for investment firms and (managers of) alternative investment funds is the broad definition of 'client' in the Wwft. This definition means that business relationships with professional counterparties (such as proprietary traders) connected to the core business of the institution also fall under the Wwft.

## 8.1 Investment firms

An investment firm may provide various investment and ancillary services and/or investment activities. An investment firm may for instance be involved directly in transaction execution or its service may consist solely of investment advice. An investment firm may also operate a trading platform such as an MTF or OTF. Despite this diversity, all investment firms qualify as institutions as defined in the Wwft and are subject to supervision by the AFM with regard to the regulations in the Wwft and the Sanctions Act.

## 8.2 Managers of alternative investment funds

The Wwft states that if an alternative investment fund or UCITS has a separate manager, the manager of the alternative investment fund is responsible for compliance with the Wwft. If an alternative investment fund does not have a separate manager, the alternative investment fund is itself responsible. Hereinafter, the responsible party is referred to as the 'manager'.

The market also features a wide variety of managers and alternative investment funds. Various parties may be involved in the distribution of participation units in alternative investment funds, such as fund managers, advisers, depositories and sub-custodians and in some situations, prime

brokers. The way in which units are offered to investors affects the extent to which the manager has or is able to obtain knowledge with regard to the client or investor.

Under European law (and therefore under Dutch law), a distinction is currently made between two types of collective investment vehicles, namely undertaking for collective investments in transferable securities (UCITS) and institutions for collective investment that do not qualify as UCITS (alternative investment fund managers, or AIFM). Among AIFM institutions, there is a further distinction between AIFMs that are required to obtain a licence and managers of alternative investment funds that are exempt from this licensing requirement (registered managers). This latter group is exempt from the licence requirement but is subject to the AFM's supervision regarding compliance with the Wwft and the Sanctions Act. In addition, some managers also offer certain investment services such as portfolio management or advice.

The manner in which an investor can acquire participating units in an alternative investment fund determines the definition of 'client'. Account has to be taken here of the determination of the relevant risks of money laundering and the manner in which the customer due diligence screening has to be performed. Although collective investment schemes are mostly focused on the medium to long term and thus possibly less interesting for money laundering purposes, they can be used for concealment in connection with money laundering or terrorist financing. The following risk-heightening aspects may be a factor:

- Participation units are usually offered on a non-face-to-face basis. Access to and transfer of units can be effected relatively simply and quickly. This makes alternative investment funds potentially suitable for concealing the source of funds;
- By extension, with a listed alternative investment fund, the units can be traded without the manager being informed at the time of or prior to the trade;
- Funds offered to single investors (such as high net worth individuals), which actually are personal investment vehicles rather than collective investment schemes.

## 8.3 Wealth management

The services of investment firms or (managers of) alternative investment funds may concern wealth management or private banking. For example, services connected with 'wealth management' may feature portfolio management and investment advice. This type of service is aimed at high net worth individuals and their families and/or businesses. These services may be particularly vulnerable to abuse by clients wishing to conceal the source of their funds or evade tax in their jurisdiction. Wealth management or private banking is cited as an increased risk in Annex III to the fourth Anti-Money Laundering Directive.

Some other risk-heightening factors include (not an exhaustive list):

- transactions and portfolios of very high value;
- complex products and services, including specific investment products;
- expectations of confidentiality and discretion;

- rich and influential clients, including clients with a public function, PEPs and clients residing outside the Netherlands;
- the use of complex structures, for instance trusts or SPVs;
- cross-border agreements involving a spread of assets across different jurisdictions with one of the institutions involved located in a country with a high risk of money laundering or a country that does not conform to international tax regulations;
- the income of clients is generated in countries and/or sectors with an increased risk of money laundering.

The account manager for these clients has an important role in the risk assessment of the client in question. Close contact by the account manager with the client makes it easier to gather information such that a fuller understanding of the nature and activities of the client and their business can be obtained (such as information on the source of the client's funds, the reasons why complex or unusual arrangements may be honest and legitimate, or the reasons why an enhanced customer due diligence screening may be appropriate).

Such close contact may however also lead to a conflict of interest if the account manager becomes too close to the client, thus detracting from the institution's efforts to manage the risk of financial criminality and breaches of integrity. For this reason, independent supervision of the risk assessment is advisable that can be carried out by the compliance function and senior management.

## 8.4 Risk factors for investment firms and managers of investment funds

The following risk-heightening factors may arise for both investment firms and managers of investment funds:

- the possibility to make payments to third parties whereby an investment account is used as a payment account;
- regular changing of payment details at the client's request;
- there is no economic rationale for the investments;
- the client wishes to purchase or sell long-term investments shortly after their initial investment, with no economic reason to do so and in particular if large losses or high transaction costs are involved.

## 8.5 Financial service providers

The Wwft applies to financial service providers providing intermediary services in life insurance and financial service providers using the National Regime (and thus qualifying as investment firms). The AFM brochure specifically dealing with compliance with the Wwft and the Sanctions Act by financial service providers is available on the AFM website (in Dutch).

*Intermediation in life insurance*

In these Guidelines, 'life insurance products and other investment-linked insurance products', as referred to in the FATF glossary, refer to agreements primarily aimed at protecting the

policyholder financially against the risk of an uncertain future event, such as death or illness. Life insurance products may also be purchased as part of an investment plan or to support pension schemes. Most life insurance products are long term in nature and some will only pay out if a verifiable event such as death or retirement occurs. Generally, the risks associated with the insurance sector are lower than for other financial products (for instance loans or payment services) or sectors (for instance banking, gambling or high-value goods). Life insurance products are offered to clients who may be either natural or legal persons. The beneficiary of the contract may be the policyholder (meaning the owner of the contract, who may or may not be the insured person), or another designated beneficiary (natural persons, legal persons or legal entities).

Life insurance intermediaries are in direct contact with their clients and are the eyes and ears of the insurance company. The intermediary thus has a very important role with respect to compliance with the Wwft.

Some risk-heightening factors include (not an exhaustive list):

- the financial service provider is confronted with the circumstance that the life insurance policy is not in the name of the actual beneficiary;
- the financial service provider encounters problems with the identification of the actual beneficiary and/or observes irregularities with regard to the name on the policy;
- the client asks the institution about paying the premium in a different way (for instance in cash);
- there is a large lump-sum payment for a policy and the source of the funds is unclear.

*National Regime*

Financial service providers using the National Regime also qualify as investment firms as defined in Section 1:1 Wft, as a result of which they are subject to the Wwft. The National Regime is described in detail in Section 11 of the Exemption Regulations under the Financial Supervision Act (Vrijstellingsregeling Wft). This states that financial service providers holding a licence for giving advice on life insurances or mortgages are exempt from the obligation in the Wft to obtain a licence to act as an investment firm. The exemption applies to the extent that the financial service providers advise on units in an alternative investment fund or UCITS or receive and transmit orders in relation to units in an alternative investment fund or UCITS. The exemption under the Wft is not relevant for the question of whether these parties are subject to Wwft. The relevant issue is whether these parties formally qualify as investment firms as referred to in Section 1:1 Wft. To the extent that these parties provide investment services, they must comply with the obligations pursuant to the Wwft.

## Part II. The Sanctions Act 1977

# 9. The Sanctions Act 1977

The Sanctions Act 1977 is a framework act and is the basis for details of national and international regulations for the implementation of international sanctions. Sanctions are political instruments in the foreign and security policy of the United Nations and the European Union. These are mandatory instruments applied in reaction to contraventions of international law or human rights, among other things.

In principle, the regulations of the European Union impose the following categories of financial or other sanctions:

- an order to freeze assets;
- a ban on the direct or indirect provision of financial resources to the persons or organisations in question;
- a ban or restriction on the provision of financial services.

## 9.1 AFM's supervision

With respect to the administrative organisation and internal controls (hereinafter: AO/IC), the reporting requirement, retention obligation and the obligation to provide information by institutions subject to the Wwft, the AFM is charged with supervision of compliance with the Sanctions Act and regulations and rulings under the Sanctions Act relating to financial transactions (hereinafter: sanctions regulations). The sanctions regulations apply to everyone. Institutions accordingly have to take measures to avoid acting in contravention of the sanctions regulations. This is a punishable offence and forms a threat to the business operation's integrity and control, and an important requirement under the Wft and for obtaining a Wft licence.

## 9.2 Compliance with sanctions regulations

An institution must ensure that it has AO/IC measures in place to ensure compliance with sanctions regulations. These measures must at least ensure an adequate control of the institution's administration with regard to the correspondence of the identity of relations with a legal or natural person or entity as referred to in the sanction regulations, with a view to freezing financial assets of this relation and the prevention of making financial assets or services available to this relation. It is important here that an institution knows the 'relations' it has in the context of the sanctions regulations, as the definition of a 'relation' is wider than that of a 'client' as referred to in the Wwft, and includes any person involved in a financial service or financial transaction. This therefore includes clients, the representatives and UBOs of clients, and also directors of parties related to a client.

*Continuous screening system*

To prevent contraventions of the sanctions regulations, the AFM recommends a continuous screening system designed to minimise the possibility of a contravention, with screening taking place, for instance at the outset, on a regular basis in the event of changes at the relation (such as

the UBO) and changes to the sanctions lists, and on termination of the relationship. The timing of the periodic screening will depend on the type of institution and the relations involved.

*Sanctions lists*

An institution has to screen its relations against the National Terrorism Sanctions List, the EU Sanctions List and the UN Sanctions List. The contents of the regulations set out the financial sanctions measures involved, the purpose of these measures and the countries, regions and persons or entities that it concerns.

The National Terrorism Sanctions List includes persons and organisations involved in terrorist activities.

On the EU Sanctions List, institutions can see which *persons and entities* have to have their assets frozen on the basis of financial sanctions regulations applying in the Netherlands. Bans or restrictions on the provision of financial services against *certain countries and regions* are not stated in the EU Sanctions List. For this information, the regulations need to be consulted directly. The official EU website www.sanctionsmap.eu can offer practical assistance for establishing whether a ban or restriction on the provision of financial services applies to certain countries or regions.

An institution also needs to be aware that sanctions measures can be circumvented, for example through the use of intermediaries located in countries not subject to sanctions, and take appropriate measures in this respect.

If you wish to be informed on a monthly basis of the status of European and national sanctions, you can subscribe to the AFM/DNB Sanctie Alert.

The AFM's web page on the Sanctions Act (https://www.afm.nl/nl-nl/professionals/onderwerpen/sanctiewet) includes links to useful documents such as the National Terrorism Sanctions List, the EU Sanctions List, the consolidated UN Sanctions List and the 'Guidelines to Financial Sanctions Regulations' issued by the Ministry of Finance in 2020.

*Reporting requirement*

If an institution establishes that the identity of a relation corresponds to a natural or legal person or entity listed in the sanctions regulations, it must notify the supervisor of this without delay by email to meldingsanctiewet@afm.nl. The institution should use the notification form available at www.digitaal.loket.afm.nl/Documents/Formulieren/meldformulier-sanctiewet.pdf. The institution should also notify the identity details of the relation in question to the supervisor. The AFM will check that the report is reasonable and will pass it on to the Ministry of Finance. Follow-up action by the AFM depends on the nature of the specific case. The AFM is authorised to pass this information on to the Public Prosecution Service (Openbaar Ministerie).

If you establish that there is a transaction or proposed transaction with an existing or new relation included in a sanctions list, in certain cases you must report this to the FIU as an unusual transaction. This is an obligation pursuant to the Wwft.

Failure to report a transaction when an institution has established that the identity of a relation corresponds to a natural or legal person or entity listed in the sanctions regulations is an economic offence as defined in Section 1(2) of the Economic Offences Act. An economic offence is a criminal offence.

*Retention obligation*

Institutions must archive their reports to the supervisor as described above, with details of the accounts of and transactions with the relations mentioned in the reports for five years after the sanctions regulation in which the natural or legal person or entity is stated is no longer in effect or is suspended.

*Cooperation with supervisory authorities*

Institutions must provide information in relation to the implementation of the sanctions regulations to the supervisory authority on request.

Classification

AFM - Publiek

The Dutch Authority for the Financial Markets

T 020 797 2000 | F 020 797 3800

PO Box 11723 | 1001 GS Amsterdam

www.afm.nl