Guidance document

Wwft BES and Sanctions Act

Explanation of the Anti-Money Laundering and Combating Terrorism Financing Act BES for

- life insurance brokers
- investment companies
- portfolio managers

September 2021

AFM

The Dutch Authority for the Financial Markets (AFM)

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.

Index

1 Introduction

Specific regulations aimed at controlling money laundering and terrorism financing risks are laid down in the Anti-Money Laundering and Combating Terrorism Financing Act BES (**Wwft BES**). The Wwft BES is an important instrument for the prevention of misuse of the financial system for money laundering and financing of terrorism on Bonaire, St. Eustatius and Saba (**the BES Islands**).

The Wwft BES contains both the obligation to carry out customer due diligence and the obligation to report an (intended) unusual transaction. The point of departure of the act is the risk-based approach to compliance and the supervision of compliance with the act and regulations based on the act. The Wwft BES prescribes, based on open norms, what the service provider must do in connection with the prevention of money laundering and financing of terrorism. It is up to the service provider to fill in these open norms in the actual compliance with this act. The Wwft BES has been amended with effect from 1 July 2021, as a result of which it now also contains a number of new obligations. In view of the amendment of the Wwft BES, the AFM has revised this guidance document to incorporate the changes and additions.The AFM has drawn up this Wwft BES guidance document to provide guidelines to the service providers on the BES Islands that are subject to Wwft BES supervision by the AFM for compliance with the obligations pursuant to the Wwft BES, and to thus promote compliance with this act.

The purpose of this guidance document is to:

- emphasise the importance of the prevention of money laundering and terrorism financing;
- provide an overview of the main obligations pursuant to the Wwft BES;
- help service providers to comply with the Wwft BES requirements by providing a practical explanation regarding a risk-based application of the measures.

This guidance document is not a legally binding document or an AFM policy rule. This document should be regarded as an explanation of the Wwft BES. This guidance document does not have the status of laws or regulations. The approach described is not necessarily the only manner to comply with the requirements pursuant to the Wwft BES. The examples presented in this guidance document are not exhaustive, cannot always be regarded as sufficient and are only intended as an illustration of a number of legal obligations. Service providers are free to comply with the requirements pursuant to the Wwft BES in another manner.

2 Combating money laundering and terrorism financing

Money laundering and terrorism financing form a serious threat to a country's economy and can impact economic growth. The absence of an effective anti-money laundering policy, that satisfies international standards, can have a detrimental effect on both domestic institutions and international trade. Moreover, criminal activities to conceal the origin of criminal proceeds or to use legal or criminal money for terrorism purposes can seriously undermine the soundness, integrity and stability of the financial sector and the confidence in the financial system as a whole. Both money laundering and terrorism financing have an impact on the integrity and reputation of the financial sector of a country as a whole and of individual financial and other service providers.

2.1 What is money laundering?

Money laundering is the carrying out of activities with the aim of concealing the origin of illegally obtained revenues. Revenues that are laundered can be obtained from various criminal activities. It can concern money obtained from fraud or theft, drug money, or money obtained from corruption or bribery. It is not always the case that it will be criminal money in the form of cash. The criminally obtained money can also (already) be in the financial system.

Money Laundering is penalized as a criminal offence in Caribbean Netherlands in the Penal Code BES in sections 435a (intentional money laundering), 435b (habitual money laundering) and 435c (culpable money laundering). Money laundering is an independent criminal offence for which the conviction of the predicate offense, such as bribery, embezzlement, fraud, drug or human trafficking is not necessary.

A service provider can also be held liable based on the Penal Code BES for culpable money laundering. This can be the case, for example, when a service provider receives, possesses or transfers funds derived from crimes or is involved in, or provides advice on financial and other transactions of such funds, while the service provider must reasonably suspect that these funds were derived from a crime.

2.2 What is terrorism financing?

Terrorism concerns, in short, threatening to commit, preparing or committing violent acts or deeds that damage or undermine society based on an ideological motive. The aim of terrorism is to bring about changes in society or to influence political decision-making.

Section 84a of the Penal Code BES sets out the criminal conduct that is regarded as a terrorism crime. The financing of terrorism has been decreed a criminal offence in section 435e of the Penal Code BES.

The financing of terrorism is in fact an umbrella term for various acts that ultimately serve to enable terrorist activities. Contrary to money laundering, the origin of the money is not really the issue, but the purpose for which the money is used and by whom the money is used. With terrorism financing, it is not only about financial support, but also, for example, supplying goods and providing services. In combating terrorism financing, the prevention of criminal offences also plays a large role due to the disruptive consequences of terrorist activities.

3 The main obligations of the Wwft BES

The Wwft is aimed at the designated 'service providers'. The scope of the concept 'service provider' is very broad. The AFM has been appointed as the supervisor for a number of types of service providers, i.e. life insurance brokers, investment firms and asset managers. This guidance document is therefore aimed at providers of the following services:

- brokerage for concluding life insurance against payment of a premium as set out in the Financial Markets Act BES (**Wfm BES**);
- operating as an investment company as defined in the Wfm BES;
- providing an investment service (portfolio management) which is defined as:
  - receiving and transmitting orders of customers with regard to financial instruments;
  - executing orders with regard to financial instruments for the account of these customers;
  - managing an individual's assets.

Service providers are the gatekeepers to the financial system: anyone who wants to carry out a financial transaction or otherwise transfer any property is reliant on service providers. The Wwft BES contains two main obligations for service providers: customer due diligence and reporting unusual transactions.

First, they must carry out customer due diligence. This means that, before they can start providing services, they must carry out customer due diligence and determine whether the customer poses a higher risk of money laundering or financing of terrorism. Obtaining knowledge and information about the customer's identity, identifying the ultimate beneficial owner and determining the purpose and the nature of a business relationship is indispensable to being able to recognise signs that could indicate money laundering, underlying criminal offences or terrorism financing. Gathering information and checking behaviour ensure that the service provider obtains a more complete image of the customer. This is of great importance for the prevention of money laundering or terrorism financing.

Customer due diligence must be carried out in a risk-based manner. This means that customer due diligence must be tailored to the risks that the type of customer and the type of service entail. Therefore, service providers are obliged to gear the measures that they take in connection with customer due diligence to the risks of the nature and size of their own enterprise and the services provided as well as to the risks of a concrete customer or transaction. To this end, service providers must gather the necessary information and ensure that they have a clear understanding of the possible risk factors. These risk factors pertain to, for instance, the type of customer, the manner of introduction of the customer, the product or transaction, and the customer's country of origin or country of residence.

The second main obligation of the Wwft BES is the reporting of unusual transactions to the Meldpunt Ongebruikelijke Transacties: the Financial Intelligence Unit-Nederland (**FIU-NL**). If a service provider qualifies a transaction as unusual, the service provider must immediately report this of their own accord to the FIU-NL. Indicators have been included in the Regulation Wwft BES for when a transaction must be qualified as unusual. The most important indicator - the suspicion of money laundering or terrorism financing - must be assessed by the service provider itself based on the transaction-specific circumstances.

4 Risk assessment (section 1.9 (new))

Service providers must perform an assessment of their own risks of money laundering and terrorism financing and they must document this risk assessment and keep it up to date. When requested, this risk assessment must be provided to the AFM. In the risk assessment, the service provider analyses the risks of money laundering and terrorism 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 service provider 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 service provider reviews what additional measures must be taken to fill the gaps. This risk assessment provides the basis for the development of the policy, procedures and measures to mitigate and effectively control the identified risks (see also chapter 5).

Risk factors

Under section 1.9 Wwft BES, a service provider must perform a risk assessment and must document the results of the risk assessment and keep this risk assessment up to date. Therefore, the risk assessment must be revised when necessary; for example, when new risks arise. When performing a risk assessment, a service provider must in any event take into account the risk factors that relate to the type of customer, product, service, transaction and delivery channel and to countries or geographic areas. Examples of these risks are mentioned below. Please note that this is not intended as an exhaustive list.

Customer risk

In mapping the customer risk, the service provider has some discretion in terms of how it weighs up relevant aspects. However, there are categories that may give rise to a higher risk and which may require the institution to take additional measures. These include, for example, high net worth individuals and customers in professions that are closely associated with money laundering and fraud, such as in the real estate sector. Other examples are customers who carry out their transactions (or arrange for their transactions to be carried out) under unusual conditions. This concerns, for example, frequently and inexplicably switching to other service providers in different geographic locations.

Product, service and transaction risk

In mapping product, service and transaction risks, the service provider likewise has some discretion in terms of how it weighs up relevant aspects. When determining such risks, a service provider can take into account aspects such as new or innovative products/services and technologies and crypto products. In addition, collaborating with other financial institutions that are based in a high-risk country can be identified as an activity with a higher risk. Cash payment of the premiums for a life insurance policy may also give rise to a higher risk.

Country risk

With regard to the country risk, the service provider takes into account countries and geographic areas that may give rise to a high risk. In assessing the country risk, an institution has some discretion in terms of how it weighs up relevant aspects. Indicators for a high country risk can include the fact that independent sources (such as Transparency International's Corruption Perception Index) identify a country or geographic areas as having a high level of corruption or other criminal activities). In performing the assessment, the service provider must in any event take into account the publications of the Financial Action Task Force (FATF), which

identify various risk countries and risk areas that have not to a sufficient extent set up a system for the prevention of money laundering and terrorism financing. The publications can be found on the FATF's website and are annually revised in February, June and October (if necessary). Service providers are expected to be aware of the contents of these publications and to take appropriate measures in response where necessary. Countries against which the UN or the EU has issued sanctions also qualify as high-risk countries.

Unacceptable risk

Service providers must develop and document a policy on how to respond in the event that customers form an unacceptable risk. If unacceptable risks are identified, the service provider is allowed to refuse to accept the customer or, where necessary, to terminate the existing relationship with the customer. To safeguard that it can properly terminate its relationships with existing customers, the service provider draws up a customer exit policy. This policy sets out the conditions under which the relationship with an existing customer is to be terminated and the procedures and timeframe for such a customer exit. Some examples of unacceptable risks are:

- (potential) relations identified on sanction lists;
- 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.

Design of the risk assessment

The steps the service provider takes to identify and assess money laundering and terrorism financing risks within its business should be appropriate to the nature and size of the service provider's business. If a service provider does not offer complex products or services and has no or limited international exposure, the risk assessment need not be that complicated or sophisticated. What matters is that the service provider transparently documents the risks it has identified and to what extent those risks are controlled by the control measures, such as by carrying out enhanced customer diligence in case of an increased risk.

When drawing up a risk assessment, it is important that risks are not defined in too general terms and that they are specifically related to the nature and size of the service provider'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 service provider's customers include any PEPs and if so, whether these PEPs are Dutch or foreign PEPs and which specific risks this creates. The service provider must make a realistic assessment of the risks. Therefore, the service provider should not automatically assess risks as low without substantiating this.

5 Policy (section 1.10 (new))

Under section 1.10 Wwft BES (new), a service provider must have in place policies, procedures and measures to mitigate and effectively control risks of money laundering and terrorism financing which are appropriate to the nature and size of the service provider's business. The service provider's risk assessment must transparently clarify the risks (under section 1.9 Wwft BES). In addition to its own risk assessment, the service provider must incorporate the national risk assessment for the BES islands (**NRA BES**)[1] in its policy. NRA BES is a national risk assessment to determine the risks of money laundering (and to a lesser extent terrorism financing) on the BES islands (see section 1.14 Wwft BES (new). The service provider must regularly review its policy, also on the basis of updates of the NRA BES.

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 categorising customers in risk categories), continuous monitoring and audits with regard to PEPs and sanction regulations. In addition, the policy should include a clear description and allocation of duties, powers and responsibilities within the service provider.

Under section 1.12 Wwft BES (new), if a service provider is part of a group, it must apply in an effective manner any group-level policies and procedures that meet the regulations laid down or pursuant to Wwft BES.

Design of operational management

Under section 1.11 Wwft BES (new), a service provider must designate the responsibility for compliance with the Wwft BES to one of the persons within the service provider who decides on day-to-day policy matters. This designated day-to-day policymaker should bear responsibility for supervising compliance with the Wwft BES within the service provider. The service provider's policies, procedures and measures should be subject to the approval of the service provider's day-to-day policymakers. In addition, where this is appropriate to the nature and size of the service provider's business, the service provider must have in place a compliance function and an audit function.

The 'nature and size' criterion concerns a combination of factors, so not only the size of the service provider in terms of its number of staff members, but also its number of customers, number of foreign or high-risk customers and types of products.

The compliance function focuses on checking compliance with the statutory regulations and the internal regulations drawn up by the institution. The obvious approach is that the compliance function carries out the risk assessment and the updating of the risk policy. Furthermore, the person responsible for the compliance function has the responsibility to report unusual transactions and to provide the required information to the FIU-NL. This means that they cannot confer with others, such as the policymaker(s), about making such a report.

In addition, provided that this is 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 BES, the audit function must independently audit the service provider's compliance with the Wwft BES, as well as the compliance function's performance of its duties.

[1] See this link to the NRA BES 2019: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjeu57GwIXxAhULA2MBHQ_7AQIQFjAEegQIBhAE&url=https%3A%2F%2Fwww.rijksoverheid.nl%2Fbinaries%2Frijksoverheid%2Fdocumenten%2Fkamerstukken%2F2020%2F07%2F03%2Fcahier-national-risk-assessment-witwassen%2Fcahier-national-risk-assessment-witwassen.pdf&usg=AOvVaw08DVqsZDD-wzNGYRpO_ez0.

6 Customer due diligence (section 2.2)

For the prevention of involvement in money laundering and terrorism financing, service providers should carry out customer due diligence on all of their customers. The Wwft BES applies an open norm for the obligation to carry out customer due diligence. This means that the act does not prescribe exactly how customer due diligence must take place, but it does state what customer due diligence must ultimately lead to.

The service provider must take reasonable measures to ensure that the data collected concerning the customer, the customer's ultimate beneficial owner and the customer's representative are correct and complete and kept up to date (section 2.3(2)). A service provider must demonstrably tailor its customer due diligence to the risk sensitivity in relation to money laundering or terrorism financing and must in this respect consider the type of customer, business relationship or transaction (section 2.2(3) (new). 'Demonstrably' means that all information that is necessary to be able to demonstrate that customer due diligence has been carried out must be documented. The service provider must also be able to demonstrate in which manner the risks of money laundering and financing of terrorism have been taken into account. A service provider is obliged to draw up a risk profile for every customer with whom it maintains a business relationship (section 2.5). The AFM expects from service providers that the substantiation why a customer has been given a specific risk profile is also apparent from the customer file.

When there are doubts about whether the earlier obtained information is truthful, additional customer due diligence must be carried out. A service provider is not permitted to enter into a business relationship or to carry out a transaction for a customer if it has not performed customer due diligence or if customer due diligence has not led to the intended result (section 2.4(2)).

If the service provider already has a business relationship with the customer and the service provider cannot satisfy certain customer due diligence requirements, the service provider terminates this business relationship (section 2.4(3)).

Which customer due diligence steps do you take?

1 Has the identity of the customer been verified? This must take place based on documents that are reliable and are from an independent source.
2 Have you determined that the person who represents the customer vis-à-vis you is authorised to do so? Have you verified the identity of the representative?
3 Do you know who has an ownership interest or control over the customer (the ultimate beneficial owner)? Have you verified the identity of the ultimate beneficial owner?
4 Do you have insight into the ownership and control structure of the customer and do you understand this structure?
5 Has the purpose and the nature of the relationship been determined? For example, do you know why the customer has contacted you and is the requested service appropriate for the customer?
6 Did you check whether the funds used in the service are derived from a legitimate source?
7 Did you draw up a risk profile of the customer in which all customer due diligence information is taken into account?
8 Do you continuously monitor the business relationship with the customer and the transactions carried out during the relationship, including an investigation into the source of funds if necessary?

6.1 Relying on another service provider (section 2.6)

Section 2.6 regulates that, under certain conditions, service providers can rely on the customer due diligence carried out by certain other service providers. A service provider may only rely on the customer due diligence that has been carried out by another service provider if it has received the relevant customer information from the other service provider. This party must be a designated service provider subject to the Wwft BES.

This section pertains to both the situation that a service provider acts on behalf of a customer at the receiving service provider as well as in the event in which a service provider introduces a customer to another service provider. The latter will certainly be the case in the event of brokers in life insurance who introduce customers to, for example, insurers and in the event of asset managers.

If the customer is introduced by another service provider, for example, a broker, the service provider adopts the customer due diligence information from the other service provider. This party must be a designated service provider subject to the Wwft BES. The introducing service provider can be lawyer, civil-law notary or junior civil-law notary established in the BES islands; or a collective investment scheme, life insurer, broker in life insurance, credit institution or money transaction office that has been issued a licence pursuant to the Wfm BES.

The customer due diligence measures of the other service providers must be of such quality that this can be relied on. As the service provider itself always remains responsible for customer due diligence, also when the due diligence or a part of it is adopted from another service provider. The service provider will thus always have to make its own risk assessment of the customer and constantly monitor the relationship (section 2.5).

6.2 Risk-based customer due diligence

The service provider must perform a risk assessment of the individual customer before entering into a business relationship or executing a transaction. It is important in this case that the service provider is aware of the risks connected to the customer, the activities, services and transactions that are executed. To this end, the service provider must draw up a risk profile of the customer and continuously keep this up-to-date. The information necessary for keeping the risk profile up-to-date is gathered while maintaining the business relationship with the customer and executing the transactions. In addition, sources such as notifications from the Financial Action Task Force (FATF) and the European Union (EU) regarding high-risk jurisdictions are also taken into account, where relevant, in determining a customer's risk profile.

If it follows from the risk assessment that there is a proven low risk, the service provider can suffice with simplified customer due diligence (see paragraph 6.9). If there appears to be a high risk then enhanced customer due diligence must be carried out (see paragraph 6.10). In the event that there is no proven low or high risk, the service provider must carry out customer due diligence in accordance with section 2.2 (see paragraph 6.4 and further). It is up to the service provider to determine the required thoroughness of the customer due diligence. This can mean that more information must be gathered.

6.3 Reason and timing of customer due diligence (section 2.3, section 2.4, section 2.7)

A service provider carries out customer due diligence if it enters into a business relationship or executes an occasional transaction for a customer in or from the BES Islands.

Customer due diligence also has to be carried out (again) if there are indications that the customer is involved in money laundering or terrorism financing; if the service provider doubts the reliability of earlier obtained information on the customer; or if the risk of involvement of an existing customer in money laundering or terrorism financing gives cause for this.

The main rule of section 2.4 is that a service provider carries out customer due diligence before it executes an occasional transaction or enters into a business relationship. Section 2.7 provides a possibility to complete customer due diligence at a later stage if this is necessary in order not to disrupt the service provision. This is only permitted if there is a demonstrable low risk and customer due diligence is completed as soon as possible after the first contact.

6.4 Identification and verification (section 2.2 (1)(a), section 2.12)

A customer is the person or entity with whom the service provider enters into a business relationship or who has a transaction executed. In the event of life insurance brokerage, as referred to in the Wfm BES, the person or entity who pays the premium as well as the person or entity to whom the benefit is paid both qualify as customers. An example of this is a company that concludes group life insurance for its employees. The company that pays the premium must be regarded as a customer. When the benefit is paid out, it has to be determined to who the benefit is paid. This is usually the employee's surviving dependants. They are then also regarded as customers. As part of the customer due diligence measures, the service provider must always verify the customer's identity.

Section 2.12 specifies the manner in which the verification of the customer's identity must take place. With regard to the verification, a distinction is made between the nature and origin of persons. The basic rule is that the verification of the identity takes place based on documents, data or information from a reliable and independent source.

Documents based on which the verification of the identity of natural persons can take place are:

- one of the following, valid documents in the country of issue:
  - a driver's licence;
  - an identity card;
  - a travel document or passport;

- the original of a valid residence permit, accompanied by a valid passport;
- a copy of a valid residence permit, accompanied by a copy of a valid passport and a statement of the competent authorities.

The verification of the identity of a legal person incorporated in accordance with the law of the BES Islands who has its registered office there or a foreign legal person who has an office on one of the BES Islands can take place based on the following documents:

- a duly authorised extract from the Chamber of Commerce;
- a deed or statement, drawn up and issued by a lawyer, civil-law notary or junior civil-law notary established in the public bodies.

The verification of the identity of a **foreign legal person** who is not established on a BES Island can take place based on the following documents:

- a duly authorised extract from the register of an institution comparable to the Chamber of Commerce;
- a statement issued by a functionary who is independent of the customer, such as a civil-law notary or a lawyer, from the country of residence, who can sufficiently guarantee the reliability of this statement based on the nature of his position.

This extract or statement must contain the following information:

- **of a legal entity:**
  - the legal form
  - the name in the articles of association;
  - the trade name;
  - the complete address;
  - the place of business;
  - the country in which the registered office is located; and
  - if the legal person is registered with a Chamber of Commerce or similar authority, the registration number and the country or island jurisdiction in which such a Chamber, or similar authority, is established.

- **of all authorised persons and representatives:**
  - the name;
  - the date of birth; and
  - the document based on which the identification has taken place.

Customer due diligence with regard to foreign legal persons could, in practice, lead to problems. As in some countries, there is no or no well-functioning trade register and also obtaining a notarial deed is not always possible or only possible with great difficulty. Therefore, a flexible approach has been chosen in which a service provider can verify the identity based on documents that are generally accepted in international commerce. A service provider will have to be able to demonstrate to the supervisor that it was justified to rely on certain documents.

6.5 Ultimate beneficial owner and ownership structure (section 2.2 (2)(b))

Part of customer due diligence is identifying the ultimate beneficial owner and taking adequate measures to verify the identity of the ultimate beneficial owner. If the customer is a legal person, the service provider must also take reasonable measures to obtain insight into the ownership and control structure of the customer.

The ultimate beneficial owner is the natural person who is the ultimate owner of or has control over a customer or the natural person for whose account a transaction or activity is carried out. The two criteria that are of importance to qualify a person as the ultimate beneficial owner concern holding the ultimate ownership of or having the ultimate control over a customer via the holding of shares, voting rights, ownership interest or other means.

A natural person must be deemed to be an ultimate beneficial owner if that person:

- directly or indirectly has formal control by holding an ownership interest of more than 25%; or
- can exercise de facto control over the relevant legal entity.

In certain cases, persons who are part of the senior management (such as directors under the articles of association or partners) are registered as so called “pseudo-UBOs”. The designation of senior management as pseudo-UBOs can take place for various reasons, including that no ultimate beneficial owner can be identified based on the shares, voting rights or ownership structure. This designation guarantees that an ultimate beneficial owner is registered for every legal entity. The designation of senior management as pseudo-UBOs is a last resort and may only take place after all possible means of identifying the ultimate beneficial owner have been exhausted and provided that there are no grounds for suspicion, or when there is doubt as to whether persons identified as an ultimate beneficial owner are in fact an ultimate beneficial owner or have control.

In this regard, the term ‘senior management’ should be understood to include the entire statutory board of the customer or all partners of a partnership.

The identification of the ultimate beneficial owner plays a role if the customer of the service provider is a legal entity. It must be clear which natural person is - ultimately - behind the legal entity. The service provider must take adequate measures to ensure that the stated identity of the ultimate beneficial owner corresponds with the actual identity as well as what the nature and size is of the ultimate interest held.

The service provider must always make an effort to verify the identity of the ultimate beneficial owner in the customer due diligence process. Verification of the identity takes place using documents, data or information from a reliable source, for example, a valid passport, a valid identity card or a valid driver's licence. The depth of the measures to verify the identity may be geared to the risk of money laundering and terrorism financing of the specific business relationship or transaction. This means, for example, that in the event of a higher risk, the service provider must base the verification of the identity of the ultimate beneficial owner on certified documents and information from a reliable and independent source. Only asking the customer who is the ultimate beneficial owner is not sufficient to verify the identity of the ultimate beneficial owner.

In the event of corporate structures, the point of departure is that the service provider knows and understands the customer's ownership and control structure. This means, for example, that in the event of a complicated structure consisting of many companies, the service provider must make more of an effort to understand the (international) structure of the customer compared to simple companies with one shareholder.

6.6 Representative (section 2.2 (2)(e)(f))

The service provider must take reasonable measures to verify whether the customer is acting for himself or for a third party. The natural person who represents the customer must also be identified and his identity must be verified.

Of the natural person who claims that he is acting as the representative of another natural or legal person, the service provider must determine whether this natural person is authorised to represent the other natural or legal person. If a natural person claims to represent a legal person indirectly, then the chain of representation authorisation must be determined. This is the case, for example, if a natural person indicates that he is acting on behalf of legal person A who in turn is the director of legal person X.

In all cases, the representative must identify himself vis-à-vis the service provider. The service provider must then verify the identity of the representative.

When a natural person states that he is acting on his own behalf, one may usually reasonably assume that this is the case. However, there are circumstances conceivable where this cannot simply be assumed, such as when there are doubts or doubts arise later regarding whether the customer is actually acting on his own behalf. Such doubt can arise if, for example, various customer due diligence data and information are difficult to reconcile. For example, if a customer's statement regarding the origin of the funds does not appear logical then this could be a reason for further investigation.

It is then possible, for example, that a customer who is a natural person is controlled by another natural person, which is also referred to as a frontman set-up. In this type of set-up, persons are used to carry out transaction on behalf of (criminal) third parties in their own name. The fact that a frontman is being used can be reason for a service provider to report this as an unusual transaction to the FIU-NL (see chapter 8).

If it is clear that a customer is acting on behalf of another person and there is a valid reason for this, then this person also qualifies as a customer and customer due diligence must also be carried out on this person.

6.7 Purpose and intended nature (section 2.2 (2)(c))

Obtaining information on the purpose and the intended nature of the business relationship is also part of the customer due diligence process. The available information regarding the purpose and nature of the business relationship is an important element of the risk assessment of the customer.

Part of the required information will usually become known during the contact before entering into the business relationship. The purpose of the business relationship will also become apparent from the services that the customer obtains. Additional questions can focus on obtaining clarity about the party making use of the service and the amounts involved in the service. The following questions can be asked: Where does the customer come from? Why has the customer come to me? What does the customer expect from me?

In the event of, for example, an international customer, or a customer who makes use of a complex structure, the service provider must look into why this customer makes use of such structures or why a foreign customer wishes to make use of a service provider on the BES Islands.

6.8 Source of the funds (section 2.2 (2)(d))

The source of the funds that are used in the business relationship or the transaction are also investigated during the customer due diligence process. This investigation focuses concretely on the source of the funds that are used for the transaction. For instance, the source of the funds could be from a salary, investments or an inheritance. The source of the customer's funds must be easily explained and the explanation must be plausible.

The service provider makes a risk-based assessment in order to determine the extent of the investigation. The service provider will carry out an investigation into how and when a payment was made, for example, whether this concerned a (large) cash payment, payment from a third party or payment by a non-affiliated foreign natural or legal person. The fact that the funds come from a regulated bank does not mean that the source is in order and that the service provider does not have to conduct its own investigation.

In order to determine the plausibility of the legal source of the funds the following combinations of indicators are relevant based on which the depth of the investigation into the source of the funds is determined, for instance:

- the amount involved in the transaction or service;
- the origin of the funds indicated by the customer;
- the customer's age and occupation or business activities;
- country of origin or destination of the funds; and
- the service provided.

6.9 Simplified customer due diligence (section 2.8 (new))

Unlike the former version, the current version of the Wwft BES does not designate any types of customers or services for which it is deemed sufficient to carry out simplified customer due diligence. A service provider may still carry out simplified customer due diligence, but only if the nature of the business relationship, transaction or customer is such that the associated risk of money laundering or terrorism financing is low.

Customer due diligence must be carried out in any event, but the intensity of the applied customer due diligence measures may be tailored to the risk associated with the type of customer, product, service, transaction and delivery channel or with countries or geographic areas. A service provider 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, a service provider can suffice by applying simplified customer due diligence measures. In doing so, a service provider should at least consider the risk factors referred to in section 7(2) of the Wwft BES Regulation, such as life insurance policies with low premiums.

Simplified customer due diligence means that the service provider must demonstrate that they have gathered sufficient information to be able to determine that simplified customer due diligence suffices. Furthermore, a service provider must take reasonable measures to ensure that the gathered information in this respect is up to date. Obviously, the risk associated with a customer may change during the business relationship, for example because the customer relocates to a high-risk country. In such cases, the service provider should review whether this requires carrying out customer due diligence as specified in section 2.2 or enhanced customer due diligence as specified in section 2.10.

If the service provider has indications that the customer is involved in money laundering or terrorism financing, simplified customer due diligence is then insufficient and customer due diligence as specified in section 2.2 or enhanced customer due diligence as specified in section 2.10 must be carried out.

Lastly, in the event of customers for which simplified customer due diligence has been carried out, a service provider must have sufficient information so that it can report any unusual transactions to the FIU-NL.

Situation with respect to current life insurance policies

Before the current Wwft BES came into effect, as a rule it was sufficient in certain cases to carry out simplified customer due diligence, such as in the case of life insurance policies with a fixed (lump-sum) premium payment. Service providers must now ascertain for their existing customers whether the relevant files meet the requirements under the current Wwft BES. If simplified customer due diligence was applied, the service provider must ascertain whether that is still permitted. This means that the service provider must take additional measures to increase its knowledge of the customers and ultimate beneficial owners in order to ascertain whether there is a low risk of money laundering or terrorism financing. In certain cases, simplified customer due diligence may no longer suffice and a reassessment of the customer file will lead to additional measures and additional customer due diligence. In cases where simplified customer due diligence is still sufficient according to the service provider, the AFM expects this to be demonstrably documented in the customer file.

6.10 Enhanced customer due diligence (section 2.10)

The service provider must carry out enhanced customer due diligence in the event of higher risk of money laundering or terrorism financing. Enhanced customer due diligence must be carried out if the nature of a business relationship or transaction represents a higher risk and when the country where the customer resides or is established or has its registered office entails a higher risk of money laundering or terrorism financing. The service provider can make use of the following public sources for high-risk countries:

Links to relevant websites with sources for high-risk countries

European regulations: https://eur-lex.europa.eu/homepage.html

EU information on AML/CFT including high-risk countries: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing_en

FATF high-risk countries: http://www.fatf-gafi.org/countries/#high-risk

EU non-cooperative tax jurisdictions: https://ec.europa.eu/taxation_customs/tax-common-eu-list_en

EU sanctioned countries: https://www.sanctionsmap.eu/#/main

UN sanctions: https://www.un.org/sc/suborg/en/sanctions/information

Transparency International:
https://www.transparency.org/news/feature/corruption_perceptions_index_2017

It is up to the service provider to determine for which transactions and business relationships enhanced customer due diligence must be applied. Based on a risk assessment prior to entering into a business relationship or executing a transaction, the service provider must determine whether that higher risk has materialised or could materialise. In determining the risks, the service provider should at least consider the risk factors referred to in section 7(3) of the Wwft BES Regulation.

In addition to carrying out customer due diligence in accordance with section 2.2 (1), (see paragraph 6.4 and following) additional and more extensive customer due diligence is carried out in the event of enhanced customer due diligence. In that case, additional information is requested about, for example:

- the origin of the funds of the customer or where necessary the ultimate beneficial owner;
- the reason for the organisational structure (in the event of a legal person);
- the underlying reason for the service.

Where relevant, the customer is asked to provide information from a reliable and independent source. This can, for instance, be the following information:

- ownership deeds;
- sales agreements;
- financial statements;
- financial information, such as salary slips;
- information from the Tax and Customs Administration;
- information from trade registers or other registers.

A more extensive examination will also take place via internet and other open sources, or information will be requested from colleagues in the customer's country of origin.

A number of risk increasing factors that could occur for life insurance brokers are (not exhaustive):

- the service provider is confronted with the circumstance that the life insurance policy is not in the name of the actual beneficiary;
- the service provider encounters problems with the identification of the actual beneficiary and/or observes irregularities with regard to the name on the policy;

- the customer asks the service provider about paying the premium in a different manner;
- a large lump-sum payment for a policy of which the source of the funds is unclear;
- the premium is paid by a third party who does not appear to have a clear relationship with the customer;
- in the event the policy is concluded in connection with a mortgage loan: a large difference between the purchase price of the property in comparison to the amount mentioned in the appraisal report.

The following risk increasing factors could occur for investment firms and asset managers (not exhaustive):

- the possibility to make payments to third parties whereby an investment account is used as a payment account;
- the regularly changing of payment details at the customer's request;
- an economic objective is lacking for the investments;
- the customer incurs losses with the investments but the customer does not care;
- the customer wishes to invest for the long term, but wants to sell the investment again after a short period without economic rationale and in particular if there are large losses or high transaction costs.

6.10.1 Customer who is not physically present (section 2.10(2))

The service provider must take extra measures if a customer is not present for the verification of his identity in order to compensate for the higher risk. The service provider can, for example, request additional documents, data or information to verify the customer's identity. This concerns documents in addition to the identity document. It can also concern a combination of various documents, for example, combinations of bank statements, utility bills, salary slips and/or employment agreements.

In the event of documents that are not issued by governmental authorities or judicial authorities, the service provider will have to question whether the documents are sufficiently reliable. Such documents will generally not be sufficient to verify the identity in an adequate manner. The service provider will also have to assess the authenticity of the documents provided. Service providers could, for example, ask the customer to have the documents certified by a civil-law notary or a lawyer.

The ‘name-number’ check as described in section 2.10(2)(c) is a method that is frequently used to verify the customer's identity. However, as pursuant to section 2.4 the customer's identity must be verified before a business relationship is entered into, the service provider must ensure that the first payment for the name-number check takes place before or at the same time as the beginning of the business relationship and the services that the customer uses. The first payment must come from an account in the customer's name at a bank in the countries of the Kingdom of the Netherlands, the United States of America or Canada.

6.10.2 PEP (section 2.10(3) (new))

There is also an increased risk for which additional measures must be taken if a customer (or ultimate beneficial owner) is a Politically Exposed Person (PEP). In contrast to the definition that applied previously, a person who resides in one of the BES islands can also qualify as a PEP (i.e. a domestic PEP). If a customer or a customer’s ultimate beneficial owner is a PEP who does not reside in one of the BES islands, they may qualify as a foreign POP. The national risk assessment for the BES islands (NRA BES) and the report on the security picture for the BES islands (Veiligheidsbeeld BES) both warn against the negative effects of (political) corruption in the Caribbean Netherlands, particularly on Bonaire and St. Eustatius. The risks of objectionable conflicts of interest are considered to be greatest among government officials, administrators and politicians. In the Caribbean Netherlands, politicians often work part-time. In addition to their political office, they often have corporate jobs and/or public roles. This means there is a broad overlap between the political and economic elite in the Caribbean Netherlands, which creates added vulnerability to conflicts of interest.

The exhaustive list of PEPs has been removed from the legislation. Consequently, it is up to a service provider to establish whether someone qualifies as a PEP. Service providers must also incorporate this in their policy and procedures. A service provider may still use the previously applicable exhaustive list, but they may not limit themselves to the PEP listed there. In addition, service providers must ascertain which persons with particular positions must be regarded as PEPs; examples include the Lieutenant Governor, Island Commissioners or local politicians.

The immediate family members or close associates of the PEPs must also be regarded as PEPs. In the event of family and close associates, this can also concern persons that (other than the PEP himself/herself) are not publicly known.

The following are regarded as immediate family members:

- the husband or wife;
- a partner that can be regarded as equal to a husband or wife based on domestic law;
- the children and their spouses or partners;
- the parents.

The following are regarded as close associates:

- a natural person of whom it is known that this person, together with a person who holds or has held a prominent public position, is the joint ultimate beneficial owner of legal entities or legal constructions or has another close business relationship with this person;
- a natural person who is the sole beneficiary of a legal entity or legal construction of which it is known that this was set up for the actual benefit of a person who holds or has held a prominent public position.

Service providers must have risk-based procedures to determine whether a customer (but in principle also an ultimate beneficial owner) is a PEP. In order to determine whether someone is a PEP, a service provider can consult public sources (such as the internet) or request information from an institution in the country where the customer in question (or ultimate beneficial owner) comes from. The FATF stipulates that additional customer due diligence must always be carried out with regard to foreign PEPs.

The decision to enter into a business relationship with a PEP must be taken or approved by the management of the service provider or persons authorised for this by the service provider. Furthermore, the service provider must check what the source is of the PEP's wealth and also of the funds that are used in the specific transaction or business relationship. In addition, the service provider must continuously monitor the business relationship with the PEP to see whether this relationship can be continued in connection with possible money laundering or terrorism financing risks. If an existing customer (or ultimate beneficial owner) becomes a PEP or turns out to be a PEP during the business relationship, the service provider should ensure that this business relation satisfies the stricter requirements that apply to PEPs within a reasonable period of time.

No method whatsoever can prevent that a service provider, in spite of reasonable and adequate measures, does not always (directly) recognise a PEP as such. In line with the risk-based approach, it is also important with regard to PEPs that a service provider makes a reasonable effort to recognise and identify a PEP. The quality of the formulated policy regarding PEPs and the execution thereof as apparent from the documentation in customer files are decisive for the question whether the service provider has acted in accordance with the statutory obligations.

If the customer or the ultimate beneficial owner of the customer is no longer a PEP, the stricter measures will continue to apply for 12 months in any case. It is in line with the risk-based approach to apply the measures afterwards until this customer or ultimate beneficial owner no longer forms a higher risk. Risk factors that are considered here are the type of position that was previously held by the PEP and the degree of influence that this person can still exercise after having held a politically prominent position.

6.11 Risk assessment of the customer (section 2.2(2)(d) in conjunction with section 2.5 (new))

A service provider is obliged to draw up a risk profile for every customer with whom it maintains a business relationship (section 2.5). To this end, sufficient information is gathered during the customer due diligence process to the extent that all relevant risk factors are identified and a total picture of the risks connected to a specific business relationship or transaction can be obtained.

In determining the customer's risk profile, a service provider must also consider the risk factors referred to in section 7(1) of the Wwft BES Regulation, namely:

1 the purpose of an account or relationship;
2 the sum of the assets deposited or the sum of the transactions executed by a customer;
3 the frequency of contacts or length of the business relationship with a customer.

The risk factors can be weighted by relative importance. A risk profile is then drawn up for the customer based on the information gathered during the customer due diligence process.

All customer due diligence elements are taken into account in this process. In the risk assessment, a number of factors are weighed, such as the customer's business activities or occupation, the country of residence or the country in which the customer and the ultimate beneficial owner are located, the reason for the requested services, and the source of the funds. Based on public sources, it must be examined for each customer whether there have been negative reports about the customer, the ultimate beneficial owner of the customer or the representative in recent years.

Based on the risk assessment, customers can be divided into, for example, the risks profiles low, normal and high.

What information should you take into account when drawing up a customer's risk profile?

- Do you know who the customer is? What are the customer's activities and business activities?
- Have you checked who the ultimate beneficial owner is?
- In which manner has the customer approached you? Has the customer been introduced by a third party?
- Do you understand the customer's ownership and control structure?
- Do you know the purpose and nature of the relationship? Do you know why the customer has approached you and is the requested service appropriate for the customer?
- Is the source of the funds plausible?
- Did you check whether there are negative reports about the customer, the representative and the ultimate beneficial owner?
- Did you check whether the customer, the representative or the ultimate beneficial owner is a PEP or is listed on a sanction list?
- Does the customer or the ultimate beneficial owner come from a high-risk country?
- Was it easy to obtain all the information about the customer?

7 Ongoing monitoring (section 2.2(2)(d), section 2.5)

Section 2.2(2)(d) stipulates that the service provider periodically checks whether the customer still fits the risk profile as it was drawn up at the beginning of the provision of the services. The service provider must continuously monitor the business relationship and the transactions executed during this business relationship. In this manner, it is ensured that the transactions correspond with the knowledge that the service provider has of the customer and the customer's risk profile and unusual transactions can be identified. After all, service providers can only identify unusual transactions when they have a clear picture of the customer in question. If it becomes apparent from certain transactions that the customer is deviating from the profile, the service provider must assess the risks in connection with this and whether the customer's risk profile has to be revised accordingly.

Independent of the customer's risk classification, as determined by the service provider, the service provider must periodically review whether the customer still meets the risk profile. In the periodical review, the service provider must examine whether (external) signals such as negative reports in the media on the customer or deviating transactions could be an indication for a change of the customer's risk profile. In addition, the customer due diligence information that was gathered must also be kept up-to-date. This obligation pertains to keeping the information up-to-date, not to the replacement of (copies of) documents. For instance, a copy of an identity document does not have to be replaced when the term of validity of the identity document has expired. It concerns keeping information that can change up-to-date, for instance, a person's country of residence or business activities.

The customer's transactions and the services provided to the customer are monitored continuously. If certain transactions do not match the risk profile that was drawn up, the service provider must assess the risks that this poses. All complex and unusually large transactions and all unusual transaction patterns that do not have an apparent economic or lawful purpose are also investigated. If such transactions occur, the whole business relationship with the customer is subject to enhanced monitoring. This also means that services provided and transactions executed previously must also be thoroughly re-examined.

The monitoring of the business relationship with the customer and the customer's transactions can be tailored to the type of relationship and the customer's risk profile. This can differ per sector and per product. For instance, for life insurance products, this could be one check a year, for example at the time of the payment of the (annual) premiums and a check when there is a change in the policy or the beneficiary.

8 Reporting unusual transactions (section 3.5)

Another important aspect of the Wwft BES is the obligation to report unusual transactions. The service provider investigates (intended) transactions to see whether these could be unusual in order to avoid facilitating money laundering. Whether a transaction has to be qualified as unusual is determined based on the list of indicators drawn up based on the Wwft BES. With the introduction of the amended Wwft BES, this list has also been amended; see Appendix A to the Wwft BES Regulation. As soon as a transaction meets one or several indicators, the service provider must immediately report the transaction to the FIU-NL.

A business relationship must also be reported to the FIU-NL if customer due diligence has not lead to the intended result or if the business relationship is terminated because the customer due diligence requirements cannot be fulfilled and there are also indications that the customer in question is involved in money laundering or terrorism financing.

It is important to state that the service providers and the persons who work for the service provider have a duty of confidentiality when a report has been filed and, if applicable, when the FIU-NL has requested additional information. It is a criminal offence to inform the parties involved in the reported transaction or third parties that a report has been made.

Based on section 3.5(1), the reporting of unusual transactions must take place immediately once the service provider has become aware of the unusual nature of the transaction. In the manner in which this is phrased, the situation is taken into account in which the service provider only discovers the unusual nature of a transaction after a longer period of time. After all, it is conceivable that following a customer's second or third transaction, the service provider begins to suspect that the customer's transactions are possibly related to money laundering or terrorism financing. Only then will the earlier executed transaction appear in another light and this will then have to be reported immediately. Of course, this is not the case for transactions that have to be reported based on objective indicators. In that case, the fact that the transaction falls within the situation described in the indicator is a direct reason for reporting it. There is an explanation on the FIU-NL website regarding the steps to take to register as a reporting entity at FIU-NL. The AFM recommends that you already register in order to be able to report any unusual transaction immediately.

Example of an unusual transaction

This concerns a term life insurance policy that is concluded via a life insurance broker in connection with a mortgage loan.

The sales price of the property in question is USD 150,000. The appraiser has determined a higher market value for this property, i.e. USD 380,000. In view of this large difference, the broker in question has another appraiser perform an appraisal. This time again, the market value is also a lot higher (close to the first appraisal value) than the sales price. The broker subsequently asks the customer about the difference between the sales price and the market value. As an explanation, the customer states that it concerns an older foreign lady who wants to sell her house quickly. The broker does not consider this explanation for the price difference plausible.

This is an example of an unusual transaction that should be reported to the FIU-NL immediately once the unusual nature of the transaction becomes known to the service provider. In this case, this is the moment when the customer provides an implausible explanation.

Other examples of possible unusual transactions for life insurance brokers

NB: No amounts are mentioned because these have to be determined by the service provider based on its own analysis.

- Lump sum high initial payments or high additional payments on the policy.
- Premium payments from a country that is designated as a high-risk country.
- Relocation of a policy holder, beneficiary or premium payer residing on a BES Island to a country that is designated as a high-risk country.
- Surrendered (single premium) insurance policies that have run for a period of less than three years with a surrendered value of [USD xx] or higher and the surrendered value equals 50% or more of the total paid-up premiums.
- The policy holder, beneficiary or premium payer is a foreign legal person or a natural person who does not reside or is not located on a BES Island.
- One-off lump sum benefits of [USD xx] or higher.
- Periodic sum benefits on an annual basis of [USD xx] or higher.
- Premium refund lump sum (not being the insured payment of premium refund) of [USD xx] or higher.
- Insurance policies that are terminated within the statutory notice period (30 days) and for which there is a premium payment or premium restitution of [USD xx] or higher.
- Pledge or collateralisation of the insurance for an amount of [USD xx] or higher, other than for a mortgage loan.

9 Other requirements

9.1 Training (section 3.12 (new))

A service provider must ensure that its employees, insofar as relevant for performing their tasks, are familiar with the provisions of the Wwft BES and that they follow periodic training that enables them to recognise an unusual transaction and to properly and comprehensively carry out customer due diligence. In addition, the day-to-day policymakers must now also follow periodic training, insofar as relevant for performing their tasks. Following training about the Wwft BES can be geared to the risks, nature and scope of the service provider. This can mean that employees of a service provider where only a few people work and that only offers services within Caribbean Netherlands have to follow a less intensive Wwft BES training than the, for example thirty, employees of a service provider that also offers services outside Caribbean Netherlands.

9.2 Registering and retaining customer due diligence information (section 2.13)

Recording information about the customer and the service is an important obligation in the Wwft BES. The customer due diligence information and information on the services must be recorded properly in order to be able to provide this to FIU-NL when a report is filed, or when complying with a request of the supervisor, FIU-NL or another detection agency.

All customer due diligence information and documents must be recorded so that the information can be retrieved (internally, but also for third parties). In order to comply with the obligation to record identity information in an efficient manner, a copy of the document based on which the identification has taken place can be recorded. If that is not possible, the information of the document based on which the identity was verified is recorded. This is the nature, the number and the date and place of issue of the document. Furthermore, the customer's name, address and place of residence or place of establishment and the nature of the service must be recorded. This information must also be recorded for the ultimate beneficial owners, representatives, the person/party in whose name a payment or transaction is executed and in whose name an account is opened, in the event that this is applicable.

The information is retained in an accessible manner up to five years after the termination of the business relationship or the execution of the transaction. The same applies to information of an executed or intended reported unusual transaction. The information that is included in the report and the confirmation of receipt of the FIU-NL are retained for a period of five years after filing the report in such a manner that the transaction in question can be reconstructed (section 3.5(3)).

10 Sanction regulations (section 3.13)

Political, economic, financial and other sanctions are imposed internationally and nationally on countries and jurisdictions, groups, entities and legal and natural persons. Examples are: North Korea because of their proliferation of nuclear weapons and Al-Qa'ida and the Taliban due to their terrorist activities. The main international sanctions that are of importance for the BES Islands are the sanctions that are imposed by the EU, often following the United Nations. These EU sanctions apply directly for all residents of the BES Islands. Based on the EU sanction regulations and the Sanction Regulation BES, financial enterprises must take the necessary measures to avoid violating international and national sanctions.

Sanctions generally consist of a prohibition to provide financial services to sanctioned persons and legal person and entities, and an order to freeze the funds of these parties. The sanctioned persons, insofar as these have been designated by the EU, are listed on the EU sanction lists.

It is in any case obligatory to check the UN, EU and Dutch sanction lists. In view of the fact that the BES Islands are geographically located near the USA, it is recommended to also screen the US OFAC sanction lists.

In addition to international sanctions, the Dutch government can also announce national sanctions that apply to the Netherlands, including the BES Islands.

Links to websites with information about sanctions

EU sanction lists: https://eeas.europa.eu/topics/sanctions-policy/8442/consolidated-list-of-sanctions_en

EU sanction countries and EU sanction regulations: https://www.sanctionsmap.eu/#/main

UN sanction lists: https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

Dutch sanction list: https://www.rijksoverheid.nl/documenten/rapporten/2015/08/27/nationale-terrorismelijst

OFAC sanction lists: https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx

10.1 Obligations of financial enterprises

Section 3.13 stipulates a reporting obligation for financial enterprises in connection with the Sanction Act 1977 and the Sanction Regulation BES. Financial enterprises must take measures to comply with the provisions of the sanction regulations. The measures to be taken must at least ensure an adequate control of the administration with regard to the identification of relations that correspond with legal and natural persons and entities 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.

The term ‘relation’ is defined as anyone who is involved in a financial service or a financial transaction. This refers to, among other persons, the customers of a service provider, the beneficiaries of a transaction or product, the ultimate beneficial owner of the financial assets, and the counterparty in a financial transaction or product. The service provider must take into account that authorised representatives may also have access to accounts and/or financial assets.

If there is a contract between a relation of the service provider and a legal or natural person or entity who is listed on a sanction list (i.e. a 'hit'), the service provider must immediately freeze the assets of this relation held at the service provider, refrain from providing any further services and report this immediately to De Nederlandsche Bank (the Dutch Central Bank, DNB). For this purpose, use is made of the Reporting format.

Contrary to the reporting of unusual transactions, these reports must be reported to the Dutch Central Bank. The reporting obligation of section 3.13 pertains to assets held at service providers that have to be frozen pursuant to the sanction regulations.

The providing of information comprises at least providing information on the relation's identity, which has been recorded by virtue of compliance with this act, a statement regarding the amount of the frozen balance, the number of the bank account, securities account or investment account as well as, insofar as applicable, a short description of the exact nature of the relationship and the name, address and telephone number of the contact person of the service provider. In addition, it must be stated based on which sanction regulation action has been taken.

In order to ensure that relevant information about the reported relation remains available at the service provider, information regarding the account and transaction details of the relation in question must be retained in addition to the details of the report. The retention obligation also implies retaining information in connection with any changes in the information because an exception applies by virtue of the sanction regulation. An example of an exception is an exemption or authorisation that was granted to debit or credit the account in question. This provision only applies to account and transaction information of relations that correspond with a legal or natural person or entity listed in the sanction regulations.

DNB can request information from a service provider regarding the compliance with this section. This power does not infringe on the powers assigned to the AFM pursuant to chapter 5 with regard to the other requirements of the Wwft BES.

This means that DNB can always request information from a service provider about frozen financial assets and transactions that have taken place. Such requests can be made during the period that the sanction regulation was in force but also afterwards. After all, after revoking a specific sanction measure, for example, the amount of frozen financial assets on an international level will often have to be determined. Therefore, it is necessary as a service provider to be able to provide information about the frozen financial assets, including transaction information, to DNB up to five years after a sanction regulation is no longer in force or has been lifted.

The Dutch Authority for the Financial Markets
PO Box 11723 | 1001 GS Amsterdam

Telephone
+31 20 797 2000
Fax
+31 20 797 3800

www.afm.nl

Follow us: →