AFM

Annex - Guideline Wwft and Sanctions Act 1977

Focus points for CASPs

Publication date: May 2025

AFM

Content

Introduction

In June 2024, the AFM has published an update of the Guideline Wwft en Sanctions Act 1977 (hereafter referred to as: Guideline). This Annex is complementary to the Guideline and is specifically intended for crypto-assets service providers (hereafter referred to as: 'CASPs'). Please note that the Dutch version of this Annex prevails.

As of December 30th, 2024, CASPs that are licensed or notified in the European market can offer the following crypto asset services[1]:

a) providing custody and administration of crypto-assets on behalf of clients;
b) operation of a trading platform for crypto-assets;
c) exchange of crypto-assets for funds;
d) exchange of crypto-assets for other crypto assets;
e) execution of orders for crypto-assets on behalf of clients;
f) placing of crypto-assets;
g) reception and transmission of orders for crypto-assets on behalf of clients;
h) providing advice on crypto-assets;
i) providing portfolio management on crypto-assets;
j) providing transfer services for crypto-assets on behalf of clients.

Crypto-assets and underlying techniques can bring innovation to financial markets. By using innovative technologies, values could be transferred global quickly. On the one hand, this could have many potential benefits, such as faster and cheaper transactions. On the other hand, because of its pseudo-anonymous nature and the ease and speed with which values can be sent anywhere in the world, crypto-assets are also attractive to criminals. Without proper regulation, crypto-assets also risk becoming a safe haven for money laundering and terrorist financing.[2]

CASPs are obliged to comply to specific Anti-Money Laundering and Countering the Financing of Terrorism (hereafter referred to as: 'AML/CFT') regulations.[3] As of February 4, 2025, CASPs qualify as 'other financial institution' as defined in the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (hereafter referred to as: 'Wwft').[4] Compliance of CASPs with the Wwft is, as per February 4, 2025, under supervision of the AFM.[5] As Wwft-institution, CASPs have certain obligations in order to prevent money laundering and terrorist financing within the financial system.

Pursuant to the Sanctiewet 1977 (Sanctions Act 1977, hereafter referred to as: 'Sanctions Act'), as per February 4, 2025, CASPs are obliged to take measures within their administrative organization and internal controls (AO/IC), in order to safeguard compliance with the provisions of applicable sanctions regulations.

[1] Article 63 and 60 MiCAR.
[2] FATF, Virtual Assets en Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing en Europol Spotlight 'Cryptocurrencies: tracing the evolution of criminal finances and National Risk Assessment Witwassen 2023, (WODC, April 3, 2024) p. 74.
[3] By Regulation (EU) 2023/1113, CASPs fall within the scope of the Anti-Money Laundering Directive (Directive (EU) 2015/849). The TFR Implementation Act implements this Regulation. Relevant for compliance with rules to prevent money laundering and terrorist financing are also the various Guidelines published by the European Banking Authority (hereinafter "EBA"). It is advisable to take note of these. This Annex cites several of these Guidelines.
[4] Article 1a(3)(k) and (l) Wwft.
[5] Article 38 TFR, Article 3(2)(g) of the Fourth Anti-Money Laundering Directive (Directive (EU) 2015/849) and Article 1a(3)(k) and (l) Wwft. For providers of crypto asset services that had a DNB registration before December 30, 2024 (hereinafter: "registrants"), they may make use of the transitional regime that applies until June 30, 2025. During the transitional period, the AFM will monitor registrants' compliance with the Wwft and Sanctions Act

In addition to the legal requirements of the Wwft and Sanctions Act, CASPs are also required to comply with the AML/CFT requirements following from the Transfer of Funds Regulation (hereafter referred to as: 'TFR').[6] For instance, CASPs must send certain transaction details along with each individual transfer of crypto-assets, also known as the 'Travel Rule'.[7] In addition, guidelines on the Travel Rule have been published by EBA.[8] An explanation of the obligation to attach information to crypto-asset transfers are included in this Annex.

Applicability Guideline

CASPs are subject to AML/CFT requirements, pursuant to the Wwft and Sanctions Act. Therefore, the entire Guideline is fundamentally applicable to CASPs, as an explanation of the Wwft and Sanctions Act.

In short, this means that CASPs can use the Guideline to fulfil the legal obligations pursuant to the Wwft and Sanctions Act, for example in the risk assessment, design of policies, procedures, group policies, execution of client investigation, reporting of unusual transactions and compliance with the Sanctions Act.

As previously mentioned, within this Annex, additional legal requirements apply to CASPs, such as the legal requirements following the TFR. The purpose of this Annex is to provide sector specific focus points for CASPs and explanatory notes on the AML/CFT requirements applicable to CASPs.[9] The Guideline and this Annex should therefore be read in conjunction.

Supervision by the AFM

The supervision of the AFM on compliance with the Wwft and Sanctions Act is risk based. Therefore, the AFM requests her supervised institutions to fill-out the Wwft/Sanctions Act questionnaire periodically. The AFM uses the information obtained via this questionnaire to prepare risk profiles of the institutions.

In addition, the obtained information provides an overall picture of the inherent money laundering and terrorist financing risks, as well as the level of control of these risks. Furthermore, the AFM can use this information within her decision-making process during the developments of the supervising strategy.

Reading guide

This Annex contains three Chapters:

- Chapter 1 covers the sector specific focus points pursuant to the Wwft,
- Chapter 2 covers the focus points pursuant to the Sanctions Act, and
- Chapter 3 provides an explanation on the legal requirements following the TFR.

[6] Regulation (EU) 2023/1113.
[7] Regulation (EU) 2023/1113.
[8] EBA/GL/2024/11, 4 July 2024, Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113 (Travel Rule Guidelines): https://www.eba.europa.eu/publications-and-media/press-releases/eba-issues-travel-rule-guidance-tackle-money-laundering-and-terrorist-financing-transfers-funds-and.
[9] For example, the Guideline also includes sector-specific concerns for investment fund managers, investment firms and financial service providers.

1. Focus points Wwft

In addition to the guidance notes regarding the Wwft, the AFM outlines specific focus points for CASPs regarding the Wwft within this chapter.

1.1. Risk assessment

As emphasized within the Guideline, the legal framework of controlling risks on money laundering and terrorist financing has a risk-based character. It is expected from CASPs that they develop an assessment of the risks they are facing, applicable to their operational activities. This means a sound risk assessment – the foundation of development of policies, procedures and measures – which is of crucial importance for ensuring compliance with the Wwft.[10] The measures that an institution should undertake to identify and assess the risks the institution is facing, must be proportionate to the nature and size of the organization.

The risk assessment should be focused on the crypto-assets services that the CASP is providing. Important is that the CASP considers the risk factors related to type of client, product, service, transaction, delivery channel or geographical locations. In this manner, the CASP will ensure to provide an accessible risk assessment of the areas with most integrity risks, as well as addressing the control measures of these risks.

When formulating integrity risks, it is expected to also consider the most recent national risk assessment (NRA) in the development of the risk assessment.[11] The increased risks related to CASPs, cause that a sound risk assessment and robust risk mitigating measures are expected from CASPs. It is of great importance that a CASP will not limit itself to abstract and general risks.

1.2. Important risk factors to consider when developing the risk assessment

When developing the risk assessment, CASPs should consider specific risk increasing factors, such as (but not limited to) being able to transfer crypto-assets directly and globally, no or limited limits on transaction volumes and value, high volatility and a certain degree of anonymity. In general, providing crypto-asset services bears an increased risk on money laundering or terrorist financing.

On January 16, 2024, European Banking Authority (hereafter referred to as: EBA) has published additional guidelines for credit- and financial institutions regarding money laundering and terrorist financing risk factors. These guidelines are applicable as of December 30, 2024 (hereafter referred to as: 'Guidelines ML/TF Risk factors').[12] These additional guidelines focus on CASPs.

[10] The obligation to identify and assess risks follows from Section 2b of the Wwft. This should at least consider the risk factors related to the type of client, product, service, transaction and delivery channel and to countries or geographical areas.

[11] 'Money laundering via provider of financial crypto services,' see: "National Risk Assessment (NRA) Money Laundering 2023, Scientific Research and Data Center (WODC), Cahier 2024-1 (available online)." The most recent NRA identified terrorism financing as one of the biggest terrorism financing threats: 'Financing through provider of 'crypto services,' see: "NRA Terrorism Financing 2023, WODC, Cahier 2024-2 (accessed online).

[12] EBA/GL/2024/01, 16 January 2024, 'Guidelines amending Guideline EBA/GL/2021/02 under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors to be considered by credit and financial institutions when assessing the risk of money laundering and terrorist financing associated with individual business relationships and occasional transactions (hereinafter "the ML/TF Risk Factors Guidelines")': Guidelines on ML/TF risk factors | European Banking Authority.

Some examples of risk-increasing factors that have been outlined by EBA are (but not limited to):

- When a lot of money is received and/or withdrawn in a short period of time where the money comes from the sale of crypto assets;
- The product places no upfront restrictions on the overall volume or value of transaction;
- A company, that has been recently established and is processing large volumes of transaction;
- Use of an IP address associated with a darknet or software that provides a high degree of anonymity or is linked to multiple users;
- When the necessary client information is not provided;
- When multiple payment accounts are used to fund the crypto-asset account;
- Transfers of crypto-assets involve jurisdictions with higher ML/TF risk;
- New distribution channels or new technology used to distribute crypto-assets, that have not yet been fully tested or that present an increased level of ML/TF risks.

If the client has complied with disclosure requirements in previous transfers of crypto assets or it involves products with limited or low transaction volumes and values, this can be risk-reducing. Another risk-reducing factor is when the nature and scope of the payment channels or systems used by the CASP are limited to closed-loop systems or systems designed to facilitate micropayments or payments from governments to individuals or from individuals to governments.

The AFM refers to the Guidelines ML/TF-Risk factors for a full overview of all risk increasing and decreasing factors. Title I of these Guidelines ML/TF-Risk factors are general. Title II is sector specific, in that respect, Guideline 21 is of importance for CASPs. The sector specific guidelines should be read in conjunction with Title I of the Guidelines ML/TF-Risk factors. The risk factors associated with type of client, product, service, transaction, delivery channel, country or geographical location.

The assessment of money laundering and terrorist financing risks are the foundation for development of policies, procedures and measures, in order to adequately mitigate and effectively manage the identified risks.[13]

1.3. Enhanced due diligence

In case of an increased risk on money laundering or terrorist financing, the CASP is obliged to perform an enhanced client due diligence[14]. The CASP will take additional measures as described in Guideline 21.12 of the Guidelines ML/TF-Risk factors. Prior to entering into a business relationship or a transaction, the CASP will execute a risk assessment to decide whether an enhanced due diligence needs to be performed. In addition, the CASP should also consider the risk factors as included in Annex III of the revised European Anti-Money Laundering Directive.[15] The CASP will document within its policy in which situations it will perform enhanced due diligence, as well as the specific enhanced due diligence measures that will be applied.

[13] Article 2c(1)Wwft.
[14] Article 8 Wwft and Title I of the ML/TF Risk Factors Guidelines.
[15] Directive (EU) 2015/849. The consolidated version can be found here: EUR-Lex - 02015L0849-20241230 - EN - EUR-Lex.

An example of a situation where enhanced due diligence should be applied, is in case when a CASP enters into a correspondent relationship[16], as well as transfer of crypto-assets from or to a self-hosted address.[17]

Transfer of crypto assets to self-hosted addresses are associated with potential high integrity risks, as, for example, the owner of the address is not always known.[18] Therefore, it is important that, when transferring crypto-assets to self-hosted addresses, CASPs will take mitigating measures. It is expected that the CASP will identify the AML/CFT risks associated with the transaction.

In case the CASP notices that the provided information regarding the originator or the beneficiary of the self-hosted address is not correct, or in case the CASP notices any unusual transaction patterns or an increased risk on money laundering or terrorist financing with transfers from or to self-hosted addresses, the CASP should apply enhanced client due diligence measures in order to adequately control the associated money laundering and terrorist financing risks.

It is expected that the CASP takes one of the following mitigating measures[19]:

- taking risk-based measures to identify and verify the identity of the originator or beneficiary of a transfer to or from a self-hosted address, or of the beneficial owner of the originator or beneficiary, including by relying on third parties;
- requiring additional information on the origin and destination of transferred crypto-assets;
- tightening the ongoing monitoring of these transfers;
- any other measures to reduce and manage the risks of money laundering and terrorist financing as well as the risk of non-execution and evasion of targeted financial sanctions and of targeted financial sanctions related to proliferation financing.

The mitigating measures should be proportionate to the identified risks.

Considering the international character of transactions of CASPs, we call attention to paragraph 5.8 of the Guideline regarding enhanced due diligence. In this paragraph, enhanced due diligence in case of transactions or business relationships with third countries is elaborated upon. Furthermore, within this paragraph (as well as paragraph 5.1) of the Guideline, remote onboarding and the EBA's 'Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849' are addressed.

1.4. Transaction monitoring and reporting unusual transactions with FIU-the Netherlands

1.4.1. Transaction monitoring[20]

CASPs are expected to give substance to the ongoing monitoring on the business relationship during the relationship as well as the ongoing monitoring of transactions executed during the business relationship.[21] It is expected that CASPs will distinguish monitoring of fiat-transactions and monitoring of crypto-assets transfers. Both situations require a transaction monitoring system. CASPs will include within their policies which tools will be used for transaction monitoring purposes, the configuration of the tool and the business rules applied (the

[16] Please refer to article 8(4) Wwft.
[17] Article 8(5) Wwft. Self-hosted address which are not linked to a CASP, or an entity not established in the Union and providing services similar to those of a CASP.
[18] Explanatory notes to the Implementation Act TFR, page 4.
[19] Article 8(5) Wwft.
[20] Transactions also refer to transfers of crypto-assets, as defined in the TFR.
[21] Article 3(2)(d) Wwft.

predefined criteria against which transactions are tested for possible unusual character) and why they are appropriate.[22]

When monitoring crypto-asset transfers, it is expected that CASPs use advanced analytical tools, in order to determine the risks associated with the transactions, as well as the ability to assess the history of transactions and potential links with criminal activities, persons or legal entities. This is in particular important in case of transactions with self-hosted addresses.[23] In principle, blockchain technology allows investigation into the origin and destination of crypto-assets. By applying blockchain monitoring during the client investigation process, the risks on money laundering and terrorist financing can be identified.

1.4.2. Reporting of unusual transactions

Table 2 of Annex I of the Wwft Implementation Decree 2018 (Uitvoeringsbesluit Wwft 2018) has been amended to list the indicators for reporting unusual transactions to Financial Intelligence Unit (FIU-the Netherlands):

Providers of crypto-asset services as referred to in Article 3, paragraph 1, subsection 16(a), (b) and (d) to (j) of the Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023	A transaction where the institution has reason to believe that this related to money laundering and terrorist financing.
Providers of exchange services as referred to in Article 3, paragraph 1, section 16, (c) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023	A transaction where the institution has reason to believe that this related to money laundering and terrorist financing. A transaction of an amount of € 10,000 or more in which an exchange takes place between virtual currencies and cash fiduciary currencies.

CASPs should be registered as reporter with FIU-the Netherlands, in order to be able to report unusual transactions without undue delay.[24] For more information, please see paragraph 6.2 of the Guideline.

The lack of information from the originator or beneficiary in crypto asset transfers may also be grounds for reporting an unusual transaction to FIU-the Netherlands. Please see paragraph 3.5 of this Guideline for more information.

[22] Article 2c(1)(2) Wwft in conjunction with article 3, paragraph 2(d), Wwft.
[23] Article 21.13 of the ML/FT Risk Factor Guidelines.
[24] Article 16(1) Wwft.

2. Focus points Sanctions Act

In addition to the Sanctions Act guidance notes that have been provided in the Guideline, within this Chapter the AFM outlines some specific focus points for CASPs regarding the Sanctions Act.

Based on article 2, paragraph one of the Regeling toezicht Sanctiewet 1977 (**RtSw**)[25], a CASP should take measures within their administrative organisation and internal control system (AO/IC), in order to ensure compliance with relevant sanctions regulations.

2.1. Risk assessment and mitigating measures

It is expected that the CASP will develop an assessment of the risk of sanctions-evasion and violating sanctions regulations, in order to address specific mitigating measures to counter these risks. In order to do so, it is important that the CASP will develop robust policies, procedures and measures. In doing so, the CASP must ensure in each case that the risk is minimal that a service or transaction will involve the transfer of financial resources to a (legal) person referred to in the sanctions regulations.[26]

The measures that should be undertaken by the CASP, should at a minimum consider screening of the business relationships of the CASPS on the sanction lists (persons and entities).[27] CASPs should apply ongoing monitoring of the business relationships, for example by having an automated (sanctions) screening system.

Another example of adopting robust measures in high-risk situations on exposure to sanctions regulations, is making use of geolocation-instruments and instruments that recognize proxy-IP-services. In this manner, the CASPS will be able to identify and prevent that her business relationships are originated from/located in sanctioned countries or countries where sanctions measures apply.[28]

Other measures in case of increased sanction risks are:

- When entering into the business relationship, obtaining relevant information regarding the activities and type of company of the business relationship, as well as the country the company is operating in and type of client of the business relationship;
- Information on the ultimate beneficent owner of the crypto-assets; and
- Obtaining detailed information from the client regarding the purpose of the crypto-assets transfer.[29]

2.2. Policies and procedures

CASPs should guarantee that the AO/IC of the CASPs will enable the CASP to comply with sectoral sanctions and sanctioned distributed-ledger-addresses.[30]

In addition, within its policies, procedures and measures, the CASP should indicate which measures will be undertaken, in case a true match is identified with a (legal) person on the sanctions list. These measures should

[25] The RtSw applies to CASPs under article 10(2)(l) Sanctions Act.
[26] Explanatory note Regulation on Supervision of Sanctions Act 1977, Government Gazette 28 September 2005, no 188, pg. 21 (para 4.3).
[27] Article 2(2) RtSw.
[28] Guidelines EBA/GL/2024/15. The guidelines were adopted on 14 November 2024 and apply from 30 December 2025.
[29] Guidelines EBA/GL/2024/15. The guidelines were adopted on 14 November 2024 and apply from 30 December 2025.
[30] Please see article 3(18) TFR for the definition.

enable the CASP to instantly freeze the assets of the business relationship mentioned on the sanctions list. Furthermore, within the policies, the CASP will elaborate on the definition of "relationship". In that respect, please see paragraph 9.2 of the Guideline for further information on the relationship definition in accordance with the Sanctions Act.

EBA's Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures[31], which are expected to be in force as of December 30, 2025, provide guidance in the design of the CASP's sanctions screening policy.

These EBA Guidelines also address the data points that CASPs should consider when executing sanctions screening, in order to assess whether sanctions restrictions apply[32]:

- Information on originator and beneficiary;
- Purpose of the transfer of crypto-assets, depending on the depending on the extent to which the institution is exposed to sanction risks, as well as other data regarding the actual sender/receiver of the crypto-assets;
- Details of the CASPs involved in the crypto-asset transfer, including intermediary institutions, correspondent relationships and screening of identification codes;
- Other details of the crypto-asset transfer, depending on nature and transaction type, the received supporting documentation, if information is available and subject to the exposure assessment of restrictive measures;
- Wallet addresses of the principal and the beneficiary of the crypto-assets, to the extent that this information is available within the public lists of wallet-addresses, linked to the restrictive measures.

2.3. Verification in case of a self-hosted address

In case the CASP executes a transaction with a self-hosted address, the risk might occur that the self-hosted address is not owned/controlled by the client itself, but by another (legal) person as described in the sanction's regulations. In case the CASP concludes that the risk that economic resources are being provided to (legal) persons as listed within the sanctions regulations are more than minimum, the CASP should verify the identity of (legal) persons owning or controlling the self-hosted address. Therefore, CASPs facilitating transactions with self-hosted addressed should at least include the following measures within the AO/IC:

- A risk assessment addressing the cases in which the risk that economic resources will be provided to (legal) persons on the sanctions list is more than minimal.
- Policies describing the situations in which the CASPs should verify the identity of the (legal) person owning or controlling the self-hosted address;
- Policies describing specifically what these verification measures entail.

2.4. Sanctions Act reports

In 2024, the Act international sanctions regulations (Wet internationale sanctiemaatregelen) were consulted by the Dutch Central Government.[33] Within this proposed Act, it is described that a central reporting point will be established. Until this establishment is final, CASPs should file their Sanctions Act reports, following article 3

[31] Guidelines EBA/GL/2024/15. The guidelines were adopted on 14 November 2024 and apply from 30 December 2025.
[32] Guide 21 of the EBA Guidelines "Guidelines on Internal Policies, procedures and controls to ensure the implementation of Union and national restrictive measures: addressed to financial institutions (EBA/GL/2024/14)": Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures | European Banking Authority.
[33] https://www.internetconsultatie.nl/sanctiemaatregelen/b1.

RtSw, with the AFM. This also applies to registrants, who formerly reported to DNB. The reporting form can be retrieved from the website of the AFM[34] and need to be submitted by sending an e-mail to meldingsanctiewet@afm.nl. Please consult the most up-to-date information regarding submittance of sanction matches reports to AFM, on the website of the AFM.

For further requirements regarding the content of the recording of policies and procedures in the AO/IC and the notification to the AFM in case of a 'sanction hit', please see section 9 of the Guidance.

[34] Sanctiewet 1977

3. Focus points Transfer of Funds Regulation (TFR)

The traceability of crypto-assets transfers can be a particularly important and valuable tool in the prevention, detection and investigation of money laundering and terrorist financing. The TFR therefore requires (intermediary) CASPs to attach information to transfers of crypto-assets and perform controls on receiving transfers so that information on the originator and beneficiary remains traceable throughout the chain of crypto-asset transfers. This is also known as the 'Travel Rule'.[35]

For payment service providers, obligations to attach information to transfer of funds already existed in the TFR to improve the traceability for the purpose of preventing, detecting and investigating money laundering and terrorist financing.[36] The revised TFR extends the scope by 30 December 2024 to include transfers of crypto-assets.

3.1. Scope of application

The TFR applies to CASPs of the originator, CASPs of the beneficiary and intermediary CASPs. In addition, the TFR applies to any transfer of crypto-assets,[37] carried out by at least one CASP established or having its registered office in the European Union.

The TFR defines transfers of crypto-assets as follows: ''any transaction with the aim of moving crypto-assets from one distributed ledger address, crypto-asset account or other device allowing the storage of crypto-assets to another, carried out by at least one CASP acting on behalf of either an originator or a beneficiary, irrespective of whether the originator and the beneficiary are the same person and irrespective of whether the CASP of the originator and that of the beneficiary are one and the same."[38]

The TFR does not apply if the originator and beneficiary are CASPs acting on their own account or in cases where individuals transfer crypto-assets without the involvement of a CASP.[39] The TFR does not include an exception for intra-group transactions.

CASPs should set out in their policies and procedures which transactions in the context of its crypto-asset services fall within scope of the TFR. Furthermore, within the policies and procedures the CASP should describe in which transactions the CASPs is the originator and in which it is the beneficiary. If any transactions in the context of the crypto-asset services provided by the CAPS do not fall within the scope of the TFR, the CASP must reflect which concrete transactions this concerns, as well as which exclusions or derogations as referred to in Article 2 TFR this concerns.

[35] The recital of the TFR shows that with the TFR, the EU is fulfilling its commitment to implement the 40 recommendations of the Financial Action Task Force (FATF), in particular with regard to recommendation 16.
[36] Regulation (EU) 2015/847.
[37] Including transfers of crypto assets, which are carried out by means of crypto vending machines.
[38] Article 1(10) TFR.
[39] For scope, please see article 2 TFR.

3.2. CASP of the originator

The CASP of the originator shall ensure adequate and verified information on the originator and beneficiary in crypto-asset transfers. Article 14 TFR requires the CASP to collect, maintain and attach information when transferring crypto-assets. The CASP of the originator shall now allow the initiation or execution of crypto-asset transfer until full compliance with Article 14 TFR is ensured.[40]

3.2.1. Information to be included about the originator

The first paragraph of article 14 TFR reflects which information the CASP of the originator should attach to the transfer of crypto-assets regarding the originator.

In any case, it should be achieved that the identity of the originator is established. At least, this should include the name and address of the originator, including the name of the country, combined with additional information. This should include a combination of the following information: the number of the official personal document and the customer identification number[41] or the originator's date and place of birth, as far as this combination leads to the identification of the originator.[42] The attachment of the date and place of birth acts as an alternative for the customer identification number.

In addition, the CASP should attach the following information of the originator of the crypto asset transfer:

- The distributed-ledger-address of the originator, in case the transfer is registered on a network making use of distributed-ledger-technologies (hereafter referred to as: DLT) or similar technology[43], as well as the crypto-asset account number of the originator, in case such an account number exists and is used to process a transaction;
- The crypto-asset account number of the originator, in case the crypto asset transfer is not registered on a network making use of DLT or similar technology;
- Provided that the necessary field exists in the template of payments messages and the originator has provided this information to its CASP, the current LEI[44], or in absence of this LEI number, any other similar, official identification codes of the originator.[45]

For crypto asset transfers, the originator's CASP verifies the accuracy of the information, in accordance with article 14(6) TFR, of the originator as mentioned in the first paragraph based on documents, data or information from reliable and independent resources. What can be considered reliable and independent resources is further elaborated upon within the Guideline.

Following article 14 (7) TFR, the verification of the identity of the initiator is exempted in case the CASP has verified the identity during the client investigation performed, in accordance with the legal obligations of the CASP following the AMLD[46]. This means that the verification of the identity is deemed to have taken place and should not be verified again.

---

[40] Article 14(8) TFR.
[41] Please see the Travel Rule Guidelines, p. 58-59, for the definition of client identification number: "Following the FATF approach, the customer identification number refers to a number that uniquely identifies the originator to the originating financial institution and is a different number from the unique transaction reference number. The customer identification number must refer to a record held by the originating financial institution which contains at least one of the following: a national identity number, or a date and place of birth."
[42] Please see Guideline 35 and further of the Travel Rule Guidelines.
[43] Please see the definition within article 3(24) TFR.
[44] *Legal Entity Identifier*, please see the definition within Article 3(23) TFR.
[45] Guideline 41 of the Travel Rule Guidelines.
[46] Article 13 and 14(5) of Regulation (EU) 2015/849.

3.2.2. Information on the beneficiary to be added

According to Article 14(2) TFR the CASP of the originator shall ensure that crypto-asset transfers are accompanied by the following information on the beneficiary:

- Name of the beneficiary;[47]
- Distributed-ledger-address of the beneficiary, in case the crypto-asset transfer is registered on a network that makes use of DLT or similar technology, as well as the crypto-asset account number of the beneficiary, in case such an account number exists and is used to process a transaction;
- The crypto-asset account number of the beneficiary, in case the crypto asset transfer is not registered on a network making use of DLT or similar technology;
- Provided that the necessary field exists in the template of payments messages and the beneficiary has provided this information to its CASP, the current LEI[48], or in absence of this LEI number, any other similar, official identification codes of the beneficiary.[49]

3.2.3. Information in case of a joint-account/address/portfolio

For transfers from a joint-account, address or wallet, the information of all account-, address-, or wallet holders should be provided. In case the transfer of the respective information cannot occur due to technical limitations as prescribed in Article 24 of the Travel Rule Guidelines, the CASP should provide the account-, address- or wallet-information of the originator that gave the assignment of the crypto asset transfer. If this information is not available the information of the primary account-, address- or wallet holder will be provided.[50]

3.2.4. Information in case of batch file transfers

In case of a batch-file transfer, it is possible for the CASP to provide all required information all at once.[51] In order for the CASP to provide this information all at once, the batch-file transfer should comply with the following conditions: (i) all transactions need to be provided in one batch file, containing all required information, (ii) each transaction included in the batch file, should contain a separate DLT-address, crypto-asset account number or unique transfer identification code and (iii) all transactions should be originating from one originator. This implies that, when the batch file contains multiple transfers, all information should be provided separately. [52]

3.2.5. When and how to attach information?

The aforementioned information regarding the originator and the beneficiary should be provided previously, simultaneously or concurrently with the crypto-asset transfer. However, it is not required that this information is attached to the transfer or included in the transfer itself. The CASP will ensure that the information is not conflicting with the provisions as set out in the General Data Protection Regulation (hereafter referred to as: GDPR). Please see paragraph 3.6 of this Annex regarding GDPR.

[47] Guideline 35 of the Travel Rule Guidelines.
[48] *Legal Entity Identifier*, please see the definition within Article 3(23) TFR.
[49] Guideline 41 of the Travel Rule Guidelines.
[50] Guideline 40 of the Travel Rule Guidelines.
[51] The information as required per article 14(1) TFR
[52] Article 15 TFR.

CASPs should use infrastructures and services for the transmission and reception information that have the technical capacity to send and receive the information completely, without omissions or errors.[53]

3.3. CASP of the beneficiary and the intermediary CASP

3.3.1. Completeness and accuracy of the information

CASPs of the beneficiary and the intermediary CASP are expected to establish policies and procedures, in order to investigate and assess whether the provided information is complete.[54] For an overview of the information to be assessed or sent along, please see the previous section. These procedures should be carried out in a risk-based manner.

3.3.2. Verification of the information

Before making the crypto-assets available to the beneficiary, the CASP of the beneficiary shall verify the accuracy of the information provided following article 14(2) TFR, based on documents, data or information obtained from a reliable and independent source.[55] Within the Guideline, the definition of a reliable and independent source is explained in further detail. Both the CASP of the beneficiary and the intermediary CASP shall not allow transfers to be carried out, in case it finds that the required information is missing or incomplete, following article 16(1)(2).

3.3.3. Execution, refusal, return or suspension

The CASP should have policies and procedures in place, based on her organizational risk assessment and risk appetite, which elaborate upon the consequences in case the CASP finds out the provided information is incomplete. Within these policies and procedures, it should at least be included in which cases the transfers will be executed, refused, returned or suspended.[56] A CASP that is monitoring real time and finds out the provided, required information is incomplete, and still decides to proceed the crypto asset transfer, is required to document on which grounds the CASP decides to proceed with this transfer. A CASP may also refuse or return a transfer and communicate the reason to the other CASP. If a transfer is suspended, the CASP shall notify the other CASP and request that CASP for the missing information.

In case the information is not provided within the defined deadline(s), the CASP should decide whether to refuse the crypto-asset transfer or carry it out. The CASP will document this decision adequately.[57] In case refusal of the transaction is technically not possible, the transferred crypto-assets should be transferred back to the originator. If returning the crypto-assets to the original address is not possible, the CASP is expected to apply alternative methods. Within its policies, the CASP will define which alternative measures should be applied in the aforementioned situation. These measures should, at a minimum, include that the returned assets are kept in a secure, segregated account while communicating with the originator about an appropriate return method.[58]

[53] By way of derogation, CASPs may exceptionally use infrastructure or services with technical limitations on data completeness until 31 July 2025, as long as these are offset by additional measures or corrections to fully comply with the Travel Rule Guidelines. These additional procedures should at least include alternative mechanisms for collecting, retaining and making available the information that cannot be transmitted to the receiving CASP in the transmission chain due to technical limitations. Please see Guidelines 21 and 24 of the Travel Rule Guidelines.
[54] Article 16(1) and 20(1) TFR. In the case of the CASP of the beneficiary, it concerns the information regarding the originator and the beneficiary as mentioned in Article 14(1) and 14(2) TFR. In the case of the intermediary CASP, it concerns the information as mentioned in Article 14(1)(a)(b)(c) and 14(2)(a)(b)(c) TFR.
[55] Article 16(3) TFR.
[56] Article 17(1) TFR.
[57] Guideline 64 of the Travel Rule Guidelines.
[58] Guideline 55 of the Travel Rule Guidelines.

In that respect, reference is made to paragraph 3.5, in which further details are given on repeatedly neglecting CASPs.

3.4. Transfers from or to a self-hosted address

3.4.1. Record in policies

In case crypto-assets are being transferred from or to a self-hosted address, particular challenges could arise in the field of identification of the originator or the beneficiary. Therefore, the TFR has addressed specific provisions which apply to transfers from or to self-hosted addresses. For the additional client due diligence measures to be applied on self-hosted address transfers, please also refer to paragraph 1.3 of this Annex regarding enhanced client due diligence.

Transferring crypto assets from or to self-hosted addresses, are associated with potential high integrity risks. CASPs should assess the risks that are associated with these transfers from or to self-hosted addresses on a case-by-case basis.[59] In addition, it is expected that CASPs will identify the money laundering and terrorist financing risks that are associated with these self-hosted addresses and that the CASP will establish policies and procedures in order to adequately mitigate the identified risks.

It is expected that the CASP will establish a risk-based procedure regarding the method of verification. Within the policies and procedures, the CASP will specify which verification method(s) will be applied. In addition, the CASP must document in this procedure which verification method it uses if one verification is not sufficient. The CASP will assess on case-by-case basis which verification method is deemed suitable, with regard to the identified integrity risks related to the client.

3.4.2. Identification of a self-hosted address

To comply with these provisions, CASPs should first identify whether or not there is a transfer of crypto-assets to and from a self-hosted address. To this end, the originator's CASP or the beneficiary's CASP should use available technical means. This includes, but is not limited to: blockchain analytics, third party data providers and identifiers used by messaging systems.[60] If such information cannot be retrieved via technical means, the originator's CASP or the beneficiary's CASP should obtain that information directly from the originator or the beneficiary.[61] The CASP should do this assessment before the transfer has taken place.

When transferring crypto-assets to or from a self-hosted address, the originator's CASP or the beneficiary's CASP should collect and maintain the information referred to in Article 14(1)(2) TFR. The CASP should also ensure that any transfer of crypto-assets can be individually identified.[62] This also applies to transfers that do not exceed the threshold of €1.000.

3.4.3. Transfer of an amount exceeding €1.000

In the case of a transfer of an amount exceeding EUR 1 000 to or from a self-hosted address, there is an additional obligation to verify whether the self-hosted address is owned or controlled by the originator or beneficiary respectively. The originator's CASP or the beneficiary's CASP should take adequate measures to

[59] In accordance with Guideline 87 of the Travel Rule Guidelines. In doing so, the CASP should apply at least one of the risk mitigation measures referred to in Article 19a(1) of Directive (EU) 2015/849 in a manner proportionate to the risks identified.
[60] Guideline 77 and further of the Travel Rule Guidelines.
[61] Guideline 78 of the Travel Rule Guidelines.
[62] Article 14(5) TFR and Article 16(2) TFR.

assess this.[63] The adequate measures should be set out in the CASP's policies and procedures. Part of the policies and procedures should also include the detection of transfers that appear to be related, thereby meeting the threshold of €1.000.[64]

CASPs should use at least one of the following verification methods when a transfer exceeds the amount of €1.000:[65]

a) Unattended verification;[66]
b) Attended verification;[67]
c) Sending a predefined amount set by the CASP, from and to the self-hosted address to the CASP's account;
d) Requesting the customer to digitally sign a specific message into the account and wallet software with the key corresponding to that address;
e) Other suitable technical means as long as they allow for reliable and secure assessment and the CASP is fully satisfied that it knows who owns or controls the address.

As previously stated, the CASP should document in its policy which verification method it will use if one verification method is not sufficient. Where the CASP is fully satisfied that the self-hosted address is owned or controlled by its customer, the CASP should document this in its systems. In these cases, the CASP is not expected to re-apply the measures above to subsequent transactions from or to the same address ('whitelisting').[68]

3.4.4. Transfer from and to third parties

When a self-hosted address is found to be owned or controlled by a third person instead of the CASP's customer, there is an increased risk of money laundering or terrorist financing. In such cases, the CASP should take additional measures for verification.[69] In addition, the CASP should also assess whether the involvement of this third person gives rise to additional money laundering or terrorist financing risks. If this is the case, it shall take additional (customer due diligence) measures to limit and effectively manage money laundering and terrorist financing risks and (when justified) report unusual transactions to FIU-the Netherlands.

3.5. Repeatedly failing CASPs and reporting obligation

The previous paragraphs describe that CASPs are obliged to share information among themselves in the cases mandated by the TFR. When information is requested by one CASP from another CASP and the CASP repeatedly fails to provide this information, there is an obligation to report this with the relevant authorities. The CASP is expected to set out in policies and procedures how it implements the obligation to report in cases of missing required information.

[63] Article 14(5) TFR jo. Article 16(2) TFR. To determine whether the value is EUR 1 000 or more, the CASP should use the exchange rate of the crypto asset being transferred to calculate its value in euros at the time of the transfer, excluding any transaction fees.
[64] Guideline 17 and further of the Travel Rule Guidelines.
[65] Guideline 83 of the Travel Rule Guidelines.
[66] As specified in the guidelines for the use of remote customer onboarding solutions pursuant to Article 13(1) of Directive 2015/849, displaying the address.
[67] Idem.
[68] Guideline 86 of the Travel Rule Guidelines. A CASP using whitelisting should have controls in place to identify changes in the ML/TF risk of the self-hosted address and its ownership or control. If the CASP determines that the ML/TF risk of the self-hosted address has changed or that there is evidence that its customer no longer owns or controls the self-hosted address, it should remove the address from its whitelist.
[69] Guideline 89 of the Travel Rule Guidelines.

First, the CASP should have effective procedures in place, based on its risk assessment, to decide the required follow-up action it should commit in the absence of required complete information. [70] When a CASP repeatedly fails to provide required information[71], an (intermediary) CASP shall directly reject any future transfers of crypto-assets to or from, or restrict or terminate its business relationship with, that CASP.[72] It may do so immediately or warn first. Defining repeated failure and how to act on it should be included in the (intermediary) CASPs policies and procedures.[73]

Repeated failure to provide required information must be reported to the AFM without delay.[74] Without delay means no later than three months after the repeated failure has been identified by the (intermediary) CASP.[75] The notification must be made regardless of the reasons justifying the breach, and regardless of whether the failing (intermediary) CASP is located in or outside the Union.[76]

Reports shall be submitted by sending an e-mail to crypto@afm.nl stating Report failure TFR.[77] The AFM requests that this e-mail be sent using Cryptshare.[78] With this report, the CASP attaches the completed report form, which can be found at Reporting obligations for CASPs.

3.5.1. Content of the report

The report should contain the following information:[79]

a) The name of the (intermediary) CASP identified as having repeatedly failed to provide required information;
b) The country in which the (intermediary) CASP is licensed;
c) The nature of the breach, including:
    i. The frequency of transfers with missing information,
    ii. The period during which the breaches were identified; and
    iii. Any reasons given by the (intermediary) CASP to justify the repeated failure to provide the required information;
d) Details of action taken by the reporting (intermediary) CASP.

3.5.2. Reporting of an unusual transaction to FIU-the Netherlands without undue delay

The lack of information from the originator or beneficiary in transfers of crypto-assets can also be grounds for reporting an unusual transaction to FIU-the Netherlands. The (intermediary) CASP itself assesses whether there is an unusual transaction, considering the criteria laid down in European law, national legislation and in their own policies and procedures. Like other Wwft-institutions, a CASP must report an unusual transaction to FIU-the Netherlands without undue delay. Paragraph 6.2 of the Guideline discusses this in more detail.

[70] Article 17(1) TFR and Article 21(1) TFR.
[71] The Travel Rule Guidelines detail the deadlines when requesting information from the failing CASP. Please see Guideline 56.
[72] Article 17(2) TFR jo. Article 21(2) TFR.
[73] Guideline 67 thru 69 of the Travel Rule Guidelines.
[74] Guidelines 74 and 75 of the Travel Rule Guidelines provide further detail on the reporting obligation, see also the remainder of this paragraph.
[75] Guideline 74 of the Travel Rule Guidelines.
[76] Guideline 74 of the Travel Rule Guidelines.
[77] The obligation to report is described in Article 17(2) TFR and Article 21(2) TFR.
[78] Secure file sharing (Cryptshare)
[79] Guideline 75 of the Travel Rule Guidelines.

3.6. Focus points GDPR

The GDPR[80] applies to the processing of personal data in transfers of crypto-assets.[81] Combating money laundering and terrorist financing is recognised as a substantial public interest. CASPs should ensure that the transfer of personal data of the parties involved in a transfer of crypto-assets is always in line with the GDPR.

CASPs often operate in multiple jurisdictions, including outside the Union. However, the CASP is obliged to always comply with its obligations under AML/CFT. Therefore, it is particularly important for CASPs operating in multiple jurisdictions to ensure that they are not prevented from passing on information about unusual transactions within the same organisation. CASPs are expected to take measures to ensure this. They should also have adequate technical and organisational measures in place to protect personal data against accidental loss, alteration, unauthorised disclosure or access.

[80] Regulation (EU) 2016/679.
[81] See among others Article 14(4) TFR.

Appendix – overview of relevant legislation

Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (TFR): Regulation - 2023/1113 - EN - EUR-Lex

EBA Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113 ('Travel Rule Guidelines'): Travel Rule Guidelines.pdf

EBA Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849: Final Amending Guidelines on MLTF Risk Factors.pdf

EBA Guidelines "Guidelines on Internal Policies, procedures and controls to ensure the implementation of Union and national restrictive measures: addressed to financial institutions (EBA/GL/2024/14)": Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures | European Banking Authority.

Not available in English:

Wwft: wetten.nl - Regeling - Wet ter voorkoming van witwassen en financieren van terrorisme - BWBR0024282

Uitvoeringsbesluit Wwft: wetten.nl - Regeling - Uitvoeringsbesluit Wwft 2018 - BWBR0041193

Uitvoeringsregeling Wwft: wetten.nl - Regeling - Uitvoeringsregeling Wet ter voorkoming van witwassen en financieren van terrorisme - BWBR0024275

Sanctions Act 1977: wetten.nl - Regeling - Sanctiewet 1977 - BWBR0003296

Regeling toezicht Sanctiewet 1977: wetten.nl - Regeling - Regeling toezicht Sanctiewet 1977 - BWBR0018806

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

Telephone
+31 20 797 2000

www.afm.nl

Data classification
AFM-Public

Follow us: →

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.