Aluehallintovirasto

Prevention of money laundering and terrorist financing

A guideline for parties subject to the reporting obligation

ESAVI/17767/2021

Supervision of businesses
06/2021 Publications of the Regional State Administrative Agencies
Regionförvaltningsverkens publikationer
10/2023, 03/2024 Updated

Table of contents

1 Purpose and target group of the guideline 5

2 The key obligations in the Money Laundering Act for the parties subject to the reporting obligation 7

3 Definition of money laundering and terrorist financing 8

4 Restriction on the scope of application of the Money Laundering Act 9

5 Risk assessment 10

6 Customer due diligence 12

6.1 Customer identification and verification of the customer's identity 14

6.2 Identifying a beneficial owner 16

6.3 Obligation to obtain information and ongoing monitoring 17

6.4 Simplified customer due diligence 19

6.5 Enhanced due diligence 20

6.6 Remote identification 20

6.7 Politically exposed persons 21

6.8 Enhanced customer due diligence that is related to high-risk states outside the European Economic Area 25

6.9. Taking sanctions regulation and fund freezing decisions into account 26

6.10 Customer due diligence data and record keeping 28

6.11 Customer due diligence measures on behalf of the party subject to the reporting obligation 30

7 Obligation to report suspicious transactions 32

7.1 Obligation to report and further inquiries 32

7.2 Form and contents of the report 33

7.3 Record-keeping and confidentiality of the data related to reports 33

8 Training and instructions 35

9 Risk management methods and reporting violations of the obligations presented in the Money Laundering Act 36

9.1 Operating principles, operating methods and supervisory measures 36

9.2 The party subject to the reporting obligation's operating methods for reporting suspected violations (whistleblowing) 37

9.3 The Regional State Administrative Agency’s system for reports concerning suspected violations 37

10 Enforcement register 39

11 Supervision and administrative sanctions 41
12 Sector-specific instructions 43
12.1 Providers of legal services 43
12.2 Financial service providers 45
12.3 Currency exchange services 47
12.4 Operators that provide ancillary services related to investment services 48
12.5 Pawnbrokers 49
12.6 Real estate and rental accommodation brokers 51
12.7 Collection agencies 53
12.8 Business service providers 56
12.9 Tax advisors 57
12.10 Accountants 58
12.11 Goods dealers 61
12.12 Art dealers 64
Additional information 69
Attached documents 70
Customer information form template 70

1 Purpose and target group of the guideline

The current Act on Detecting and Preventing Money Laundering and Terrorist Financing (444/2017, available in Finnish and Swedish, and hereinafter referred to as the Money Laundering Act) entered into force on 3 July 2017. The purpose of this Act is to prevent money laundering and terrorist financing, to promote their detection and investigation and to reinforce the tracing and recovery of the proceeds of crime.

This guideline goes through the obligations in the Money Laundering Act that have been prescribed for those parties who are subject to the reporting obligation. The purpose of this guideline is to clarify the obligations laid down in the Money Laundering Act and to be of practical help. However, this guideline is not suitable as the sole instruction for a party subject to the reporting obligation. Instead, operators must prepare guidelines on customer due diligence and the prevention of money laundering and terrorist financing based on their own risk assessment.

The term "party subject to the reporting obligation" refers to the actors who, according to chapter 1, section 2 of the Money Laundering Act, fall under the Act's scope of application. The guideline is intended for parties subject to the reporting obligation who are supervised by the Regional State Administrative Agency. They include:

- businesses and professions that provide legal services (excluding attorneys-at-law) in transactions related to certain economic activities or assets
- companies providing financial services that are not subject to the supervision of the Finnish Financial Supervisory Authority
- operators that provide ancillary services related to investment services
- pawnshops referred to in the Pawnshops Act
- real estate agencies and housing rental agencies referred to in the Act on Real Estate Agencies and Housing Rental Agencies
- holders of licences for the collection of debts referred to in the Act on Debt Collection Licences
- trust or company service providers (later, business service providers)

- parties providing direct or indirect tax advice services or taxation-related support as their primary form of business or their primary profession
- businesses or professions performing external accounting functions
- businesses or professions dealing in goods, to the extent that payments are made or received in cash in an amount of EUR 10,000 or more in total, whether the transaction is executed in a single operation or in several operations that are linked
- businesses or professions dealing in works of art, to the extent that payments are made or received in an amount of EUR 10,000 or more, whether the transaction is executed in a single operation or in several operations that are linked.

Next, this guideline summarises some key obligations under the Money Laundering Act and explains what is meant by money laundering and terrorist financing. This is followed by a more detailed discussion of the obligations and compliance with these. At the end of the guideline, there are sector-specific instructions with relevant elaborations.

In addition, the Regional State Administrative Agency has issued a separate guideline on reporting suspicious transactions and preparing a risk assessment. Links to these instructions are at the end of this document under Additional information.

2 The key obligations in the Money Laundering Act for the parties subject to the reporting obligation

1. Identify and assess the risks associated with money laundering and terrorist financing in the context of your business and prepare a risk assessment on these.

2. Update the risk assessment regularly.

3. Identify your customers and verify their identity. Also identify all customer representatives and verify their identity and ensure the agent's right to act on behalf of the customer.

4. Identify the beneficial owners of your business customers, i.e. the owners of the company and those who control the company.

5. Know your customers and their activities. Continuously monitor their activities to detect suspicious transactions.

6. Report any suspicious transactions you observe to the NBI's Financial Intelligence Unit. Even when you have opted out of a customer relationship or transaction due to its suspicious nature, report this.

7. Prepare a guideline and train your employees to comply with the obligations laid down in the Money Laundering Act.

8. If necessary, register to the anti-money laundering register kept by the Regional State Administrative Agency.

9. Create an internal, independent channel through which your employees can report violations to the provisions laid down in the Money Laundering Act that they have observed.

3 Definition of money laundering and terrorist financing

Money laundering refers to measures aimed at concealing or covering up the origin of assets acquired through crime. Money laundering is preceded by a so-called predicate offence to acquire the assets that will be laundered. Thus, in money laundering, suspicion is focussed on the origin of funds. Funds that are to be laundered could originate from any kind of crime. In Finland, most laundered money comes from property offences, financial crime, such as accounting offences, fraud or drug-related crime. The focus of money laundering could be assets acquired through crime, a benefit produced by crime or assets that have replaced them.

A typical feature of money laundering is changing the form of the asset to hinder the detection of its criminal origin. When money laundering is successful, the asset will seem like it has been legally acquired. A person is guilty of money laundering when they receive, use, convert, transfer, convey, transmit or possess assets acquired through crime with the intention of they themself or a third party benefiting from the assets or when they conceal and disguise the criminal origins of the assets.

Under chapter 32, sections 6 to 10 of the Criminal Code of Finland (39/1889), money laundering is a punishable act.

Terrorist financing refers to activities that provide or collect funds for a terrorist offence or for the financing of an individual terrorist or group of terrorists. In terrorist financing, the suspicion is focussed on the intended target of the funds, not the origin of the funds. Funds used for terrorist financing can also originate from legitimate sources. The funds may also consist of several small individual amounts. The crime of terrorist financing can be committed by someone who directly or indirectly gives or collects funds to finance terrorist acts or who knows that these funds will be used to commit terrorist offences, or to fund terrorist groups or terrorists as defined in legislation.

The financing of a terrorist offence is punishable under chapter 34a, section 5 of the Criminal Code, the financing of a terrorist under section 5a and the financing of a terrorist group under section 5b.

4 Restriction on the scope of application of the Money Laundering Act

A restriction on the scope of application of the Money Laundering Act is provided for when the activities otherwise covered are occasional or very limited, and all the following conditions are met at the same time:

- the activities are limited and the individual fees paid for them do not exceed EUR 1,000
- the activity is not the primary business activity of the person, and is an ancillary service directly related to it, whose share of turnover for the accounting period is no more than five percent
- the person carrying out the activity does not carry out any of the activities covered by the Money Laundering Act as their principal business, and
- the activity is offered to clients of the primary business activity and it is not offered generally to the public at large.

These conditions are very strict, and cases in the scope of the restriction are therefore rare. Activities may not be excluded from the scope of the Money Laundering Act just because the activities are economically insignificant, there is a small number of customers or the service is provided occasionally.

In addition, activities subject to the Money Laundering Act should be ancillary to other business activities in order to be considered within the scope of the restriction. For example, as the principal business activity, a party providing a property manager service may also offer accounting services as a small-scale ancillary service that can, if all the above conditions are met, be excluded from the Money Laundering Act. However, usually the entire business of a small accounting firm or a sole trader consists solely of accounting services, in which case the above conditions are not met. In this case, the Money Laundering Act and all its obligations will apply.

5 Risk assessment

A risk-based approach is essential when it comes to money laundering and terrorist financing. In the **risk-based approach**, the parties subject to the reporting obligation identify, evaluate and understand the risks associated with money laundering and terrorist financing that they are subjected to in the course of their activities and then scale the preventive measures required by law in accordance with the risks that they face.

Despite the challenges related to the detection of money laundering or terrorist financing, the parties subject to the reporting obligation may in many ways influence their own level of risk related to money laundering and terrorist financing and in how attractive both the sector and even an individual company can seem from the perspective of money laundering and terrorist financing. The prerequisites for effective and appropriate prevention of money laundering and terrorist financing are based on an understanding and analysis of risks. Therefore, the basis for risk-based activities is a written risk assessment prepared by the party subject to the reporting obligation, which guides its own activities.

The **risk assessment** is an up-to date description of the risk environment and risk factors affecting the party's own operations. It provides a reasoned view on how products and services offered by a party subject to the reporting obligation can be used in money laundering or terrorist financing. This is a free-form assessment, and its form, length, or method of drafting are not laid down in law. In determining the sufficient extent and coverage of the risk assessment, the party subject to the reporting obligation must nonetheless take into account the nature, size and extent of its activities. In addition, the Regional State Administrative Agency notes that pre-prepared, identical risk assessment templates created for large masses do not meet the requirements set for the risk assessment in the Money Laundering Act, but only serve as a template for the assessment of a party subject to the reporting obligation.

The risk assessment must always be based on a careful assessment of the reporting party's own activities, services, customer relationships and operating environment. The risk assessment also describes the methods used by the party subject to the reporting obligation to manage money laundering and terrorist financing risks and assesses their impact. The risk assessment includes a justified assessment of any remaining risk and whether the residual risk is acceptable, or whether the party subject to the reporting obligation must take measures to reduce and manage the residual risk.

The risk assessment may, for example, assess which types of transactions should be given particular attention, which types of customer relationships

should be subject to an enhanced customer due diligence procedure or in which customer relationships the risk of money laundering and terrorist financing is considered to be so low that the party subject to the reporting obligation could follow a simplified customer due diligence procedure. The operating principles, operating methods and supervisory measures must be monitored and developed actively and be approved by the upper management of the party subject to the reporting obligation.

Based on the risk assessment they have prepared, the parties subject to the reporting obligation can plan proportionate policies, procedures and supervision to reduce and manage the risks of money laundering and terrorist financing, and allocate their resources appropriately.

The risk assessment must be updated on a regular basis. The risk assessment must be updated, for example, when there are changes in the activities or customer base of the party subject to the reporting obligation or to the legislation they must abide by. The risk assessment and the changes to it must be submitted to the enforcement authority upon request and without undue delay.

The Regional State Administrative Agency has published a guideline on how to prepare a risk assessment for the parties subject to the reporting obligation under its supervision. The instructions describe in detail the conditions set for risk assessment and risk-based activities. The link to the risk assessment instructions is listed on the Regional State Administrative Agency website and at the end of this guideline.

The following list presents some examples of risk factors typical in all sectors:

- remote identification and its vulnerability (e.g. back-to-back electronic identification)
- virtual currencies
- cybercrime
- one-off customer relationships
- use of cash
- unclear and complex transactions and commissioning relationships
- pooled accounts.

6 Customer due diligence

Chapter 3 of the Money Laundering Act contains the provisions on customer due diligence. The key objective of the Money Laundering Act is to have all parties subject to the reporting obligation be aware of who their customers are and what they do to the extent that they are able to detect any unusual transactions. The party subject to the reporting obligation may not have anonymous customers.

The term **customer** refers to a natural or legal person to whom the party subject to the reporting obligation offers their services or who requests or uses the services provided by the party subject to the reporting obligation. A customer can be for example a person or a company. As a rule, a customer is a client or contracting partner to whom the party subject to the reporting obligation offers goods or services. The sector-specific instructions include additional information on how to define a customer if the sector involves special features that the party subject to the reporting obligation must take into account.

Customer due diligence means comprehensive knowledge of the customer. Customer due diligence includes the following obligations:

- the obligation to identify customers and verify their identity
- the obligation to identify the customer's representative and verify their identity
- the obligation to identify the customer's beneficial owners and, if necessary, verify their identity
- the obligation to evaluate whether an enhanced due diligence process should be applied to a customer relationship
- the obligation to obtain information on the activities of a customer or their beneficial owner, monitor the customer's activities and investigate the backgrounds of any unusual transactions
- the obligation to comply with sanctions regulation and decisions on freezing funds.

The measures related to customer due diligence must be observed using a risk-based approach for the entire duration of the customer relationship. Depending on the field of business that a party subject to the reporting obligation operates in, such factors as customer composition, the services and products offered, as well as geographical operating areas can vary from party to party. The objective is to allow the parties subject to the reporting obligation to scale the operating and risk management measures that are

related to their customer relationships on the basis of the risks that they have identified in relation to the special features of their customers and the services that they use. In connection with the risk-based evaluation of customer relationships, the party subject to the reporting obligation must evaluate, for example, whether an enhanced due diligence process should be used in a customer relationship.

The following list presents some examples of risk factors typical in all sectors that apply to customers:

- the customer refuses to verify their identity
- the information provided by the customer conflicts with customer data, customer profile or customer behaviour
- the customer tries to use a false or counterfeit identification document (e.g. identity theft)
- the documents and reports required for customer due diligence are incomplete
- there are ambiguities in the customer's activities and ownership structures or the structures cannot be easily determined
- the customer's contact details or company management change frequently
- the transaction acquired/sold/concluded contradicts with the financial situation of the customer
- the customer executes several transactions/commissions within a short period of time
- the customer's transactions are economically unprofitable or otherwise irrational
- the customer sells/redeems a transaction/an object it has executed soon often at a loss
- transactions are executed on behalf of the customer by non-related persons
- the customer's representative changes without any documents proving right to represent being presented
- the customer seeks out complex ownership or commission relationships
- the customer or their business has an interface with countries and regions with different geographical risks

- the customer, their family member or partner is a politically exposed person.

At a more general level, there may also be a risk that the human resources of the party subject to the reporting obligation are too small or incorrectly scaled or that the party subject to the reporting obligation has not adequately ensured that their employees are trained in compliance with the Money Laundering Act and the provisions issued under it.

Customer due diligence measures are also closely connected to sanctions regulation and regulation on the freezing of funds. For more information on the obligations related to fund freezing decisions and financial sanctions, see chapter 6.9.

If the party subject to the reporting obligation is not able to fulfil the obligations related to customer due diligence, said party may not establish a customer relationship, perform transactions or maintain a business relationship.

6.1 Customer identification and verification of the customer's identity

Chapter 3, section 2 of the Money Laundering Act contains the provisions on customer identification and identity verification.

Identifying a customer means investigating the identity of a customer in a free-form manner on the basis of the information provided by the customer. The identification process can be completed with steps such as asking for the customer's name.

Verifying the identity of a customer, on the other hand, refers to the verification of a person's identity with a document that has been provided by a reliable and independent source.

The verification document can be a valid driver's licence, identification card, passport, Kela photocard, alien's passport or refugee travel document that has been issued by a Finnish authority. If no documents that have been issued by a Finnish authority are available, the verification process can also be completed using a foreign passport or some other type of identification card that can be used as a travel document.

In the case of a legal person, an extract from the trade register or some similar type of extract from a public register can be used as the verification document. Any natural persons acting on behalf of a legal person must also be identified, their identity verified, and their right to represent said legal person must also be verified.

According to the Money Laundering Act, the party subject to the reporting obligation must identify their customer and verify their identity when establishing a regular customer relationship. The term **regular customer relationship** refers to a relationship that is of a permanent nature or that at the moment of contact can be assumed to become permanent or to a customer who has signed at least one agreement or commitment with the party subject to the reporting obligation. Some examples of situations where this type of customer relationship is established include opening an account, subscribing to a fund unit, or signing a brokerage or commission agreement.

For example, in expert services, a regular customer relationship can also concern a customer who has only one commission agreement or other commitment with the party subject to the reporting obligation. In expert services, due diligence must therefore also be extended to customers who only perform a one-off transaction with a party subject to the reporting obligation.

Under the Money Laundering Act, the party subject to the reporting obligation must additionally identify their customers and verify their identity if their customer relationship is of an irregular nature and:

1) the sum of a transaction amounts to EUR 10,000 or more, whether the transaction is carried out in a single operation or in several operations which are linked to each other
2) the sum of a sale of goods transaction amounts to EUR 10,000 or more in cash, whether the transaction is carried out in a single operation or in several operations which are linked to each other or
3) the transaction is suspicious.

An occasional customer referred to in the Act may be, for example, a customer at a jewellery store who makes a one-off cash payment exceeding the EUR 10,000 threshold.

A customer must also always be identified and their identity verified if the party subject to the reporting obligation has reason to doubt the reliability or adequacy of the information used to previously verify a customer's identity.

If a person is acting on behalf of a customer (**representative**), the representative must also be identified and their identity verified. The party subject to the reporting obligation must also confirm that the representative has the right to act on behalf of the customer. For example, if a person acting on behalf of a company acts as the company's representative, the identity of the representative must be verified, and it must be confirmed that they have the right to represent.

As a rule, a customer must be identified and their identity verified when establishing a customer relationship, and this identification and verification process must be completed by the time that the customer is to be granted control over the funds or other assets involved in the transaction or before the transaction has been completed. In case of a situation where the customer must be identified on the basis of the combined value of the transaction, their identity must be verified when the limit of EUR 10,000 is reached.

6.2 Identifying a beneficial owner

In short, the term **beneficial owner** refers to such natural persons who, through their ownership, voting rights or some other basis, can exercise control over a legal person. The beneficial owner is always a natural person.

The party subject to the reporting obligation must identify their customer's beneficial owners and, if necessary, verify their identity. The political exposure of beneficial owners must also be determined, and it must be ensured that the beneficial owners are not subject to sanctions. The risk assessment of the party subject to the reporting obligation should contain information on the situations and customers for which the identity of the beneficial owners must be verified. In addition, adequate, detailed and up-to-date records must be maintained of the customer's beneficial owners.

The beneficial owner of a corporation, such as a limited liability company, refers to a natural person who ultimately:

1) owns more than 25% of the legal person's shares either directly or indirectly or otherwise owns a similar share of the legal person
2) holds more than 25% of the legal person's voting rights either directly or indirectly, and these voting rights are based on ownership, membership, the articles of association, a partnership agreement, or some other set of corresponding rules or
3) otherwise exercises actual control over the legal person.

An indication of **direct ownership** is when a natural person owns more than 25% of the legal person under review.

An indication of **indirect ownership** is when:

1) a legal person, where one or several natural persons exercise decision-making autonomy, and own more than 25% of or has more than 25% of the voting rights in the legal person under review or
2) a natural person or legal person, where a natural person exercises decision-making autonomy, has the right to appoint or dismiss a

majority of the members of the board of directors or a corresponding body of the legal person under review, and these rights are based on ownership, membership, the articles of association, a partnership agreement, or some other set of corresponding rules.

The beneficial owners of a corporation must always be identified, no matter whether their ownership is direct or indirect. For example, if the ownership of a legal person is chained so that a limited liability company is owned by another company, the party subject to the reporting obligation has to determine the ownership chain. The chain must be determined so far back that it is possible to identify the persons who are considered to be the beneficial owners or to establish that the criteria for a beneficial owner are not met. If the beneficial owner cannot be identified or the aforementioned prerequisites are not met, the board of directors, general partners, the executive director or some other person in a similar type of position in the legal person under review will be considered the beneficial owner. In these situations, the board, the responsible partners or the managing director of the customer company must be identified. However, this derogation does not apply to such situations where a customer refuses to disclose information on any beneficial owners, while it does apply to such situations where the beneficial owner cannot be identified on the basis of ownership or voting rights.

Chapter 1, section 7 of the Money Laundering Act includes some minor derogations that are related to the question of who is to be considered the beneficial owner of entities such as foundations or limited liability housing companies. For example, the beneficial owner of a limited liability housing company are the members of the board entered in the Trade Register. Even in the cases specified in section 7, the beneficial owners must always be identified.

The identification and verification of the identity of the shareholders in an estate must be carried out to the same extent as for the beneficial owners.

In addition to identifying the beneficial owners of their customers, the party subject to the reporting obligation must also remember to register its own owners and other beneficial owners in the trade register. For more information on the registration obligation for beneficial owners and examples of actual beneficial owners, please see the Finnish Patent and Registration Office website.

6.3 Obligation to obtain information and ongoing monitoring

In addition to the identification and identity verification process, the parties subject to the reporting obligation must familiarise themselves with their

customers' activities to the extent that will allow them to be able to detect any irregular activities. Chapter 3, section 4 of the Money Laundering Act contains provisions on the obligation to obtain information and ongoing monitoring that the parties subject to the reporting obligation must comply with.

The obligation to obtain information means that the parties subject to the reporting obligation must obtain information on their customers' and their beneficial owners' transactions, the nature and extent of their business and the grounds for the use of a service or product. The party subject to the reporting obligation must have a clear understanding of how the products and services that belong to their business are used as well as what their customers' business activities comprise, how these activities are carried out, and the extent of these activities. The amount of information that is needed and the sources for said information are to be decided on the basis of the risk assessment that has been prepared by the party subject to the reporting obligation.

A party subject to the notification obligation must **monitor their customer's activities**. The monitoring must be adequate in view of the nature and extent of the customers' transactions, the durability and length of the customer relationship, and the associated risks to ensure that the transactions being conducted are consistent with the party's experience and knowledge of its customers and their business. In practice, the purpose is to have the parties subject to the reporting obligation monitor their customers in a way that they are adequately prepared to detect any deviations from the norm in their customers' activities. In a regular customer relationship, any unusual behaviour can be detected when it is compared to a customer's previous activities, while in irregular customer relationships, unusual transactions are often related to transactions that are not typical for the field of business in question.

Pursuant to the obligation to obtain information, the party subject to the reporting obligation must also pay particular attention to transactions that differ from the norm in terms of structure, size or in terms of the size or location of the party subject to the reporting obligation. The deviation can be compared with the customer's normal operations or in relation to the normal transactions in the sector of the party subject to the reporting obligation. In the same manner, the party subject to the reporting obligation must take into account the transactions that have no apparent economic purpose or that are inconsistent with the parties' experience or knowledge of their customers. If necessary, the source of the funds that are involved in the transaction must be investigated.

The reliable identification of a customer may require the utilisation of several of the aforementioned methods or the acquisition of further information

from other sources. In addition, the party subject to the reporting obligation must make sure that the necessary information acquired for customer due diligence, such as information on the customer's transactions, the nature and extent of their business and the grounds for the use of a service or product, are available.

In connection with the obligation to obtain information, the party subject to the reporting obligation must also take into account any international sanctions regimes as well as national regulations concerning the freezing of funds for the prevention of terrorism. For more information on the obligations related to fund freezing decisions and financial sanctions, see chapter 6.9.

6.4 Simplified customer due diligence

If, on the basis of its risk assessment, the party subject to the reporting obligation estimates that a customer relationship or individual transaction carries a low risk of money laundering or terrorist financing, the party may utilise the simplified customer due diligence procedure.

In the simplified procedure, the party subject to the reporting obligation can carry out the following obligations presented in chapter 3 of the Money Laundering Act in a simplified manner:

- identifying the customer and their representative and verifying their identity
- identifying and verifying the beneficial owner
- obtain customer due diligence data, carry out ongoing monitoring and obtain information on suspicious transactions and
- keeping a record of customer due diligence data.

Be aware that the simplified customer due diligence procedure does not allow for non-compliance with these provisions. The purpose is to simplify the procedure, and this simplification can apply to such areas as the amount of customer due diligence data that is required, the sources used or the timing of the verification of a person's identity. What is most important is that the simplified procedure can be justified in the risk assessment of the party subject to the reporting obligation.

The party subject to the reporting obligation must also in these situations arrange for an adequate amount of monitoring for the customer relationship so that it can detect any exceptional or unusual transactions.

Even if, the party subject to the reporting obligation determined in its risk assessment that a simple due diligence procedure was sufficient to identify a particular customer group or transaction, the simplified customer due diligence procedure may not be followed if the party subject to the reporting obligation observes transactions that deviate from the customer's normal operations or cause suspicion.

6.5 Enhanced due diligence

If, on the basis of the risk assessment prepared by the party subject to the reporting obligation, the customer relationship or an individual transaction involves a higher risk than usual of money laundering or terrorist financing, the enhanced customer due diligence procedure must be applied to the customer relationship. The same must be done if a customer or transaction has a connection with a country whose anti-money laundering and counter-terrorist financing system, according to the Commission 's assessment, poses a significant risk to the EU' s internal market or does not fulfil international obligations.

The enhanced procedure means that the party subject to the reporting obligation must pay greater attention than normally to the customer, their business activities and/or their transactions to ensure that the customer relationship does not involve any money laundering or terrorist financing.

The enhanced customer due diligence procedure can involve for example paying special attention to the verification and reliable documentation of the customer's identity, assessing the background and purpose of the customer's transactions, determining the source of their funds and monitoring the customer relationship.

The enhanced procedure must also be utilised in cases that involve remote identification or politically exposed persons.

6.6 Remote identification

Remote identification applies to situations where the customer is not present when they are being identified and their identity is being verified. In such cases, to reduce the risk of money laundering and terrorist financing, the party subject to the reporting obligation is required to:

1) verify the customer's identity by obtaining additional documents or information from a reliable source

2) ensure that the performance that is connected to the transaction is made from a credit institution's account or is paid to an account that has been previously opened in the customer's name or

3) verify the customer's identity by means of an identification device referred to in the Act on Strong Electronic Identification and Electronic Signatures (617/2009), a qualified certificate for electronic signatures referred to in Article 28 of EU Regulation 910/2014 on electronic identification and trust services, or by some other means of electronic identification that ensures information security and is verifiable.

When obtaining information, the party subject to the reporting obligation must carefully assess the adequacy and reliability of the information. Verifying a customer's identity in a sufficient manner may require a combination of several different methods and requesting additional information from several different parties.

When the customer is identified via a video connection this is also considered remote identification. If a customer displays their identity document through a video, the party subject to the reporting obligation must obtain any additional information it deems necessary to verify the customer's identity. In this situation, the identity document alone is not a sufficient means of verifying identity.

An example of a method that is considered sufficient is where the customer sends a copy of their identity document and presents the same document via video connection. In addition, the customer also provides other documents, such as register extracts or minutes, or they are obtained from other sources, such as the Trade Register.

If the party subject to the reporting obligation uses remote identification, it must address the risks and risk management methods related to remote identification in its risk assessment. The party subject to the reporting obligation must have access to remote identification procedures where attention is paid to the requested information and its adequacy.

6.7 Politically exposed persons

Chapter 3, section 13 of the Money Laundering Act includes provisions on enhanced customer due diligence in respect of a politically exposed person. According to the provision, the parties subject to the reporting obligation must have the appropriate risk-based procedures in place to determine whether a customer or their beneficial owner is or has been a politically

exposed person (PEP), a family member of a politically exposed person, or an associate of a politically exposed person.

Definition of a politically exposed person

Politically exposed persons are people who have been entrusted with considerable public authority. According to the Money Laundering Act, a politically exposed person is a natural person who is serving or has served in public office as:

a) a head of state, head of government, minister, vice or deputy minister

b) a member of parliament

c) a member of a governing body of a political party

d) a member of the Supreme Court, the High Court's Constitutional Court or a similar legal body whose decisions cannot be appealed except in exceptional circumstances

e) a member of the Court of Auditors and the highest decision making body that audits state finances corresponding to the Finance Inspectorate

f) a member of the Board of the Central Bank

g) an ambassador or chargé d'affaires

h) an officer in the armed forces holding the rank of general or higher

i) a member of the administrative, management or supervisory bodies of a wholly state-owned or state majority-owned enterprise or unincorporated state enterprise in a company other than a company whose securities are admitted to trading on a regulated market referred to in chapter 1, section 2 of the Act on Trading in Financial Instruments, or

j) a director, vice director and member of the board of an international corporation.

Government decree 610/2019 provides a detailed list of the significant public tasks listed above.

The term **family member of a politically exposed person** refers to the politically exposed person's:

a) spouse or a type of partner comparable to a spouse in national law

b) child, as well as said child's spouse or aforementioned type of partner

c) parents.

The term **associate of a politically exposed person** refers to:

a) all natural persons who are known to be the true joint and beneficial owners of corporations or entrepreneurs or legal arrangements or who are known to have any other type of close business relationship with a politically exposed person or their family member

b) all natural persons who are the true exclusive owner and beneficial owner of such corporations or entrepreneurs or legal arrangements, and it is known that these have actually been established for the benefit of a politically exposed person or their family member.

The person is known to be in a close business relationship when the connection is generally known.

When a person ceases to be entrusted with prominent public functions, the obliged entity shall take into account the ongoing risk related to the person in question for at least 12 months and apply appropriate risk-based measures until the person in question is no longer deemed to be subject to risks related to a politically exposed person.

Identification of politically exposed persons

The enhanced customer due diligence that is connected to politically exposed persons is based on international efforts to prevent corruption. Being in a position of significance and authority is associated with the risk of misuse. Therefore influential people are at a higher risk of being party to crimes of bribery or corruption. This, in turn, increases the risk that the person will attempt to hide the benefits that they have incurred from the crime. The requirements that concern politically exposed persons are of a preventive and not criminal nature, and should not be interpreted in a manner that would suggest that all politically exposed persons are involved in criminal activities. Therefore, any categorical refusals to engage in customer relationships with politically exposed persons cannot be considered acceptable.

According to the Money Laundering Act, the parties subject to the reporting obligation must have risk-based procedures in place to determine whether a customer or their beneficial owner is a politically exposed person or the family member or associate of such a person. The PEP status of board members does not need to be established unless they are considered to be beneficial owners of the customer. In addition, the political exposure of a customer's representative does not need to be determined, unless the representative is also a beneficial owner at the same time.

If, on the basis of the risk assessment made by the party subject to the reporting obligation, the customer relationship or individual transaction involves a higher risk than usual of money laundering or terrorist financing, the person's political exposure must always be determined.

The party subject to the reporting obligation can thus compare and contrast the procedure with the risks of money laundering and terrorist financing that they estimate to be related to their customer relationships and activities. The party subject to the reporting obligation should take into account what was stated above on bribery and corruption crimes, among other factors. Their procedures can thus differ between different customers, customer groups, products or services, as the associated risks can vary between groups.

The methods that the party subject to the reporting obligation uses to determine a customer's PEP status can be chosen by the party itself. At its simplest, the matter can be enquired from the customer directly. If the party subject to the reporting obligation has no reason to doubt the veracity of the response received from the customer, the party subject to the reporting obligation may rely on a report provided personally by the customer. In addition, the determination of a customer's PEP status can utilise the information available on different media channels, commercial databases as well as any potential databases maintained by different states. Pay special attention to the veracity and reliability of each information source. The measures used to determine a person's PEP status must reflect the risks at hand. The investigation of a customer's PEP status must be documented, for example as a note in the customer's customer data.

Special attention should be paid to any business relationships with such persons who have some clear connection to countries where bribery is a widespread phenomenon. For more information on the corruption levels of different countries, see Transparency International's annual index on the International corruption perceptions website.

Enhanced due diligence of a politically exposed person

If the customer or the customer's beneficial owner is a politically exposed person or a family member of such a person or a person known to be an associate of such a person:

a) the upper management of the party subject to the reporting obligation must approve the initiation of a customer relationship with such a person

b) the party subject to the reporting obligation must carry out the appropriate measures to establish the source of wealth and funds that are involved in the customer relationship or transaction

c) the party subject to the reporting obligation must arrange for the enhanced and ongoing monitoring of the customer relationship.

Enhanced monitoring can mean, for example, a more frequent customer data update schedule, acquiring information from several reliable sources and/or a more thorough investigation of the politically exposed person's liabilities or the types of business activities that they carry out.

6.8 Enhanced customer due diligence that is related to high-risk states outside the European Economic Area

The enhanced customer due diligence procedure is also required in such cases where the party subject to the reporting obligation conducts transactions or performs payments that are related to states outside the European Economic Area that have been classified by the European Commission as high-risk states for money laundering and terrorist financing. In such cases, the party subject to the reporting obligation is required to:

1) obtain further information on the customer and their beneficial owner

2) obtain further information on the purpose of the business relationship that is to be established

3) obtain further information on the origin of the funds and wealth of the customer and their beneficial owner

4) obtain further information on the reasons for the transactions

5) seek the approval of the upper management of the party subject to the reporting obligation for the initiation and continuation of the customer relationship

6) arrange for the enhanced and ongoing monitoring of the customer relationship by increasing the number and rate of inspections and by selecting the areas of business that are to be inspected in further detail.

In addition, the party subject to the reporting obligation must apply the following procedures when they are deemed necessary in a risk-based assessment:

1) the party subject to the reporting obligation must apply other necessary enhanced customer due diligence procedures

2) the party subject to the reporting obligation must utilise the necessary transaction reporting methods

3) the party subject to the reporting obligation must limit its customer relationships and transactions with customers from high-risk states.

The regulatory authority has powerful measures at its disposal to prevent the risk of money laundering and terrorist financing in connection with high-risk states. If it is necessary for the prevention of money laundering and terrorist financing, the regulatory authority can, for example, prohibit a party from establishing a subsidiary or branch in Finland or prevent a party subject to the reporting obligation from establishing a branch in a high-risk state.

See the European Commission website for more information on countries where the risk of money laundering is higher. The Financial Action Task Force (FATF) also publishes a list of high-risk countries on its website. The FATF's black list of high-risk countries includes countries with serious strategic shortcomings in the fight against money laundering and terrorism. An enhanced procedure must be used with customers and transactions related to these countries and customer relationships must be seriously considered. In turn, the FATF's grey list includes countries that actively seek to remedy their strategic shortcomings in the area of money laundering and terrorist financing. In its risk assessment, the party subject to the reporting obligation must take into account possible links with the grey list countries.

6.9. Taking sanctions regulation and fund freezing decisions into account

Under chapter 3, section 16 of the Money Laundering Act, the party subject to the reporting obligation must have effective policies, procedures and internal control to ensure that the party subject to the reporting obligation complies with the obligations resulting from sanctions regulation and decisions to freeze funds.

Sanctions regulation refers to decrees issued under Article 215 of the Treaty on the Functioning of the European Union and government decrees referred to in sections 1 and 2a(1) of the Act on the Fulfilment of Certain Obligations of Finland as a Member of the United Nations and of the European Union (659/1967). In practice, international sanctions refer, for example, to the suspension of economic or commercial cooperation with a particular country or specific groups. In sanctions matters, the responsible authority is the Ministry for Foreign Affairs, and the Regional State Administrative Agency does not publish sanctions lists or provide extensive guidance related to sanctions.

Decisions on freezing funds refers to decisions issued by the National Bureau of Investigation under the Act on the Freezing of Funds with a View to Combating Terrorism (325/2013). The National Bureau of Investigation maintains a public list of decisions on freezing funds (the "frozen funds list").

While, the obligation to comply with sanctions legislation and national decisions on freezing funds applies to everyone, and it is not a new obligation in itself, the explicit obligation introduced in the Money Laundering Act to include compliance with sanctions regulation and fund freezing decisions in customer due diligence is new and entered into force on 31 March 2023. As a result of this reform, the Regional State Administrative Agency supervises that the parties subject to the reporting obligation supervised by the Regional State Administrative Agency have appropriate procedures to ensure that sanctions regulation or regulations on the freezing of funds are not violated. The enforcement authority may impose an administrative penalty on a party subject to the reporting obligation for their lack of practices and procedures even when the non-compliance has not resulted in an actual breach of sanctions legislation or decisions on freezing funds. Taking sanctions and frozen funds lists into account is an absolute part of customer due diligence and cannot be bypassed by any means, such as on the basis of a risk assessment carried out by the party subject to the reporting obligation.

The Money Laundering Act requires that the party subject to the reporting obligation has practices and practical procedures to ensure that a transaction does not involve persons or entities subject to sanctions and that the product or service itself is not subject to sanctions. The party subject to the reporting obligation must arrange effective means to detect parties subject to sanctions. The party subject to the reporting obligation must comment on the applicable procedures in their internal guidelines. Each operator should pay attention to having written guidelines and to training their employees. In addition, the party subject to the reporting obligation must have internal control to ensure compliance with sanctions regulation in practice as well.

In practice, compliance with sanctions regulation is ensured by means of sanctions monitoring where the party subject to the reporting obligation compares the name list of the sanctions list and the national frozen funds list with its customers and other parties related to transactions. Although parties outside a contractual relationship are not usually considered to be customers of a party subject to the reporting obligation, in order to ensure compliance with sanctions legislation, other parties related to a transaction must also be identified with sufficient reliability. If sanctions monitoring is only targeted at an operator's own customers, the party subject to the

reporting obligation could unknowingly participate in a transaction where one party is a person subject to sanctions.

The Money Laundering Act does not impose methodological requirements on the means of sanctions monitoring; instead, the party subject to the reporting obligation can choose how to arrange the monitoring. Sanctions monitoring can be manual or it can be implemented by means such as with a commercial service provider's information system. When arranging procedures, the party subject to the reporting obligation must pay attention to the adequacy of sanctions monitoring and its temporal dimension. Sanctions monitoring must be carried out both when establishing a customer relationship and during an ongoing customer relationship. Sanctions monitoring must be targeted at existing customers whenever the sanctions list and frozen funds list are updated.

If a party subject to the reporting obligation identifies a person or corporation among its customers or their beneficial owners that is on the frozen funds list or the sanctions list, any ongoing transactions must be suspended and no funds may be released to such persons or corporations. The Helsinki Enforcement Office must be notified of the matter without delay by email at helsinki.uo(at)oikeus.fi. You can also contact the Helsinki Enforcement Office in situations where it is unclear if a party who is your customer is the same as the person whose funds have been frozen or is subject to sanctions. Funds belonging to a person or corporation on the list of frozen assets or the sanctions list must also not be released to a third party without the permission of the authorities.

6.10 Customer due diligence data and record keeping

Chapter 3, section 3 of the Money Laundering Act obligates the parties subject to the reporting obligation to ensure that their documents and records concerning customer due diligence are up-to-date and pertinent. The records must be stored in a secure manner for a period of five years following the end of a regular customer relationship or after an occasional transaction whose value amounts to at least EUR 10,000 has been carried out. This five-year period is the minimum duration, and in some cases there may be justifiable grounds for an even longer storage period. The records can be kept in, for example, a customer register or some other similar system used by the party subject to the reporting obligation where their storage can be considered to have been implemented in an adequately secure manner when it comes to the information security of said records.

The following customer due diligence data must be kept:

1) the name, date of birth and personal identity code

2) the representative's name, date of birth and personal identity code (however, in the case of a public guardian, instead of the name, date of birth and personal identity code of the guardian, the identification data of the service provider, the title of the guardian and, if the service provider has more than one public guardian, the serial number of the guardian shall be retained)

3) the legal person's full name, registration number, date of registration and registration authority and, if necessary, the articles of association

4) the full names, dates of birth and citizenships of the members of the board of directors or a corresponding decision-making body of the legal person

5) the legal person's field of business

6) the beneficial owner's name, date of birth and personal identity code and, if necessary, a more detailed description of the ownership and control structure

7) the name of the document used in the identity verification process, the document's number or other piece of identification data, and the body that issued the document or a copy of the document, or, if the customer has been identified remotely, information on the method or sources used in the verification process

8) the information on the customer's transactions, the nature and extent of the customer's business, their financial status, the grounds for the use of transactions or services and information on the source of funds, as well as other necessary customer due diligence data

9) the necessary information that has been obtained to meet the requirements laid down in the Money Laundering Act on the obligation to obtain information and the enhanced customer due diligence procedure that is related to politically exposed persons

10) the number of the bank account or payment account, the name of the person who owns or has the right to access the account, and the date that the account was opened and closed, as well as other identification data that is related to the account to the extent appropriate and that has not been included in the data listed above and

11) information that has been obtained through electronic identification methods and verification processes.

If the customer does not have a Finnish identity code, the aforementioned records must also include information on the customer's citizenship and their travel document data.

The party subject to the reporting obligation must inform their customers that their customer due diligence data and other personal data can be used for the purposes of preventing, exposing and detecting money laundering and terrorist financing, as well as for referring any matters concerning money laundering, terrorist financing or crimes used to obtain assets or criminal proceeds for the purposes of money laundering or terrorist financing for further investigation.

Customer due diligence information or other personal data that has been obtained only for the purposes of preventing and exposing money laundering and terrorist financing may not be used for purposes that are not compatible with these purposes.

6.11 Customer due diligence measures on behalf of the party subject to the reporting obligation

The obligations related to customer due diligence may be fulfilled on behalf of the party subject to the reporting obligation by another party subject to the reporting obligation referred to in the Money Laundering Act or by a corresponding actor who has been licenced by or is registered in another EEA state (**third party**) if this party is subject to the same types of obligations related to customer due diligence and record keeping presented in the Money Laundering Act and the party's compliance with these is monitored.

However, the use of a third party to identify a customer will not remove the responsibility of the party subject to the reporting obligation in compliance with the provisions of the Money Laundering Act. In other words, the party subject to the reporting obligation may outsource the performance of that obligation, but not the responsibility for proper compliance. The party subject to the reporting obligation must ensure that the third party delivers the information referred to in chapter 3, section 3, subsection 2, paragraphs 1–7 of the Money Laundering Act. The party subject to the reporting obligation must also ensure that all customer due diligence information is available to the party subject to the reporting obligation and that it is provided by the third party at the request of the party subject to the reporting obligation. The party subject to the reporting obligation must continuously monitor customer relationships in which the customer due diligence obligations have been carried out by a third party.

The Money Laundering Act does not regulate what kind of parties can be issued the duty of performing customer due diligence measures **on the**

basis of a contractual relationship (so-called outsourcing of services or using a representative). Chapter 3, section 7 of the Money Laundering Act does not apply to outsourcing and representative relationships when the outsourcing service provider or representative can be considered part of the reporting obligation on the basis of a contractual relationship. In other words, a party that is not subject to the reporting obligation may also take due diligence measures on behalf of the party subject to the reporting obligation on the basis of a contractual relationship.

7 Obligation to report suspicious transactions

7.1 Obligation to report and further inquiries

Chapter 4 of the Money Laundering Act contains the provisions on the obligation of the party subject to the reporting obligation to report any suspicious transactions to the Financial Intelligence Unit.

A **suspicious transaction** refers to a customer's unusual transactions whose actual purpose or objective could not be established, and customer transactions that, even after investigation, appear unusual without proper justification. A transaction may for example be suspicious because of its financial value for the customer in question, or it may otherwise be unusual in nature or deviate from typical payment transactions. A suspicion may also arise when a customer does not want to submit requested documents or if the documents appear to be counterfeit.

The party subject to the reporting obligation must pay attention to any unusual transactions and, if necessary, investigate the source of the funds related to the transaction. After the party subject to the reporting obligation has detected the suspicious transaction and fulfilled its obligation to obtain information, said party must notify the Financial Intelligence Unit without delay of the suspicious transaction or suspected case of terrorist financing. The report concerning the suspicious transaction must be submitted irrespective of whether a customer relationship has been established or refused, or whether the transaction was carried out, suspended or entirely denied.

The party subject to the reporting obligation may also submit a report for any suspicious individual payments or other performances that exceed the maximum threshold amount set by the party or for several connected payments or performances.

A transaction must be suspended for further inquiries if the transaction is suspicious or if the party subject to the reporting obligation suspects that the funds involved in the transaction are to be used for terrorist financing or a punishable attempt to finance terrorism. Alternatively, the party subject to the reporting obligation may also refuse the transaction.

Occasionally, suspending a transaction may not be possible or its suspension would hinder the process for investigating the beneficial owner of the transaction. In such cases, the party subject to the reporting obligation may complete the transaction.

The Regional State Administrative Agency has published a separate instruction for reporting suspicious business transactions. The instructions give a detailed definition of the concept suspicious transactions and provide both

general and sector-specific examples of risk indicators related to customers and transactions.

7.2 Form and contents of the report

Operators should have a low-threshold policy for reporting suspicious transactions (with a money laundering report) with care and without delay to the Financial Intelligence Unit of the National Bureau of Investigation. The report is filed electronically with the Financial Intelligence Unit's web application. For a special reason, the report may also be submitted using some other encrypted connection or secure channel. A money laundering report is not a report of an offence, and evidence is not required to support the report.

The report concerning the suspicious transaction must include the relevant customer due diligence data as well as the information on the nature of the transaction, the amount and currency of the funds or other assets included in the transaction, the origin or target of the funds or other assets, and the reason that made the transaction seem suspicious, as well as whether the transaction has been carried out, suspended or denied.

More information on submitting notifications on suspicious business transactions is available on the Financial Intelligence Unit website.

The party subject to the reporting obligation must provide the Financial Intelligence Unit with all of the information and documents necessary for the investigation of the suspicious transaction, and this must be done free of charge. The party subject to the reporting obligation must also respond to any inquiries sent by the Financial Intelligence Unit within a reasonable deadline that is set by the Unit.

7.3 Record-keeping and confidentiality of the data related to reports

The party subject to the reporting obligation must retain the necessary information obtained for the purpose of fulfilling the reporting obligation and the related documents for a period of five years. This type of data includes for example customer due diligence data as well as any other information that has been obtained by the party subject to the reporting obligation over the course of the fulfilment of its obligation to obtain information.

The data and documents obtained for the purposes of submitting a report of a suspicious transaction must be kept separate from the customer

register (or similar type of system) and they may not be used for any other purpose than what is prescribed in the Money Laundering Act.

The data and documents must be removed five years after the customer relationship has ended or the suspicious transaction has been carried out, unless their further retention is necessary for the purposes of a criminal investigation, a pending judicial proceeding or for securing the rights of the party subject to the reporting obligation or the persons employed by said party. The need to keep records of the data and documents must be reviewed no later than three years after the previous date on which this need was reviewed. An entry must be made on the review proceedings and its date.

The data subject, i.e. the customer of the party subject to the reporting obligation, does not have the right to inspect the data or documents gathered to fulfil the reporting obligation or the data or documents gathered to fulfil the obligation to obtain information laid down in chapter 3, section 4(3) of the Money Laundering Act. At the request of the data subject, the Data Protection Ombudsman may examine the lawfulness of the data on the data subject.

The party subject to the reporting obligation may not disclose a report on a suspicious transaction or related clarification to anyone, including the party subject to the notification or a person employed by the company subject to the reporting obligation. The name and identity of the person submitting a report are also confidential information.

8 Training and instructions

Chapter 9, section 1 of the Money Laundering Act contains the provisions on the training and protection of employees as well as the creation of operating instructions that are applicable to the activities of the party subject to the reporting obligation.

The party subject to the reporting obligation must draw up instructions on procedures for customer due diligence that are suitable for their own activities. Similarly, instructions must be drawn up on the acquisition of information on the customer, the continuous monitoring of the customer and obligation to obtain information related to the prevention of money laundering and terrorist financing as well as on compliance with the reporting obligation. You can use this Regional State Administrative Agency guideline when planning your own operating instructions, but every party subject to the reporting obligation must, on the basis of their risk assessment, select those procedures compliance with which will ensure compliance with the obligations laid down in the Money Laundering Act, as well as the procedures that correspond to the risks that are associated with their activities.

In addition, the party subject to the reporting obligation must ensure that its employees are provided with proper training in order to ensure compliance with the provisions of the Money Laundering Act and any provisions issued on the basis of it. The party subject to the reporting obligation must pay attention to the adequacy of the training. For example, if the party subject to the reporting obligation finds shortcomings in its compliance with the obligations laid down in the Money Laundering Act, more training is required. Records must be kept of the date, content and participants of the organised training so that the party subject to the reporting obligation is able to monitor the adequacy of the training and the fulfilment of the training obligation. By documenting the details of the training, the party subject to the reporting obligation can, if necessary, also demonstrate to the enforcement authority that it has fulfilled the statutory training obligation.

The party subject to the reporting obligation must also ensure that it protects those employees who submit reports to the FIU.

9 Risk management methods and reporting violations of the obligations presented in the Money Laundering Act

9.1 Operating principles, operating methods and supervisory measures

According to the Money Laundering Act, the party subject to the reporting obligation must have an adequate set of operating principles, operating methods and supervisory measures at its disposal, while taking into account the nature, size and scope of its activities, to reduce and effectively manage any risks related to money laundering and terrorist financing. The operating principles, operating methods and supervisory measures must include at least the following:

1) development of internal operating principles, operating methods and supervisory measures

2) internal inspection, if this is reasonable on the basis of the nature and size of the activities of the party subject to the reporting obligation.

The party subject to the reporting obligation must draw up operating principles, operating methods and supervisory measures and monitor and develop related measures. When the party subject to the reporting obligation is a legal person, the board of directors, general partner or another person in a similar position in senior management must approve the aforementioned and monitor and develop the related measures.

These operating principles and operating methods include, for example, practices related to risk management, customer due diligence and identification, reporting, record keeping, internal supervision as well as employee background checks.

The party subject to the reporting obligation must also appoint a person from its management who will be responsible for the internal supervision of its compliance with the provisions presented in the Money Laundering Act and the provisions issued on the basis of it. The party subject to the reporting obligation must appoint a person responsible for compliance if it is justified when taking into account the size and nature of the party subject to the reporting obligation.

9.2 The party subject to the reporting obligation's operating methods for reporting suspected violations (whistleblowing)

Chapter 7, section 8 of the Money Laundering Act lays down the obligation of the parties subject to the reporting obligation to define the operating procedures that the persons under their employ or its agents can follow to report through an independent channel any suspected cases of violations of the provisions and regulations issued in and on the basis of the Money Laundering Act that have occurred within said party.

The purpose of the system is to ensure that, in regard to any possible cases of non-compliance, information can be confidentially passed on within the party subject to the reporting obligation to parties such as the company's upper management or internal inspections so that the deficiencies can be handled at the earliest possible stage. Evidence of the suspected violation is not required to submit a report, and reasonable doubt is enough.

The personal data of the person who submitted the report and the party that is being reported are confidential, and the party subject to the reporting obligation must implement the appropriate and adequate measures to protect those who submit reports.

Pre-existing systems can also be used for submitting reports on any suspected cases of violations. When creating your operating methods, remember to focus on the rights and duties of the person submitting the report and the person who is being reported, the contents of the report, the procedures used to process and investigate reports, as well as other possible measures.

9.3 The Regional State Administrative Agency's system for reports concerning suspected violations

The Regional State Administrative Agency for Southern Finland also has a system that it can use to receive reports of suspected violations of the provisions in the Money Laundering Act.

As a rule, the Regional State Administrative Agency's system can be used in place of an internal system by those parties subject to the reporting obligation who are under the supervision of the Regional State Administrative Agency and meet one of the following criteria:

- they employ at most five people or their

- organisational structure does not enable the arrangement of an independent channel in the manner meant by the Money Laundering Act.

However, the party subject to the reporting obligation must also always justify the use of the Regional State Administrative Agency's reporting system in its risk assessment.

A notification of a suspected violation must be made through the Regional State Administrative Agency's e-service. The report can be submitted anonymously and must contain the following information:

- The party subject to the reporting obligation that the suspected violation concerns – name and possible business ID, sector and business location as well as other received identification and verification data.

- A description of the manner in which the reporting party suspects the provisions have been violated and when the suspected infringement has taken place or, whether the procedure is ongoing.

All suspected violations that are reported to the Regional State Administrative Agency will be taken into account as part of the enforcement authority's risk-based supervision process. The party that reported the suspected violation will not be notified of any supervisory measures that are carried out on the basis of the report.

10 Enforcement register

The Regional State Administrative Agency for Southern Finland maintains an anti-money laundering register for enforcement purposes. The purpose of the register is to improve enforcement of the prevention of money laundering and terrorist financing. It also facilitates the dissemination of instructions and bulletins to parties subject to the reporting obligation.

All the parties subject to the reporting obligation who are under the enforcement of the Regional State Administrative Agency must be registered in some business enforcement register. If the party subject to the reporting obligation has already registered with another Regional State Administrative Agency's enforcement register, they do not need to apply for inclusion in the anti-money laundering register. These operators include debt collection agencies, brokerage companies for real estate and rental apartments and pawnbrokers, which are listed in their own authorisation list.

The obligation to register in the ant-money laundering register applies to:

- providers of legal services
- companies providing financial services
- currency exchange services
- operators that provide ancillary services related to investment services
- trust or company service providers
- providers of tax advice or tax support by way of principal business or profession
- accountants
- goods dealers
- parties who sell art.

The sector-specific instructions contain more detailed information on sector-specific specifications.

The party subject to the reporting obligation must apply for inclusion in the anti-money laundering register within 14 days of entering the Act's scope of application. The application for inclusion in the anti-money laundering register must be submitted using the electronic form in the Regional State Administrative Agency's e-service.

The registration obligation applies to every company or private trader offering the aforementioned services with its own business ID, regardless of whether the companies belong to, for example, the same group or the same person.

In their application, the applicant shall declare its main business activity on the basis of which the applicant is subject to the reporting obligation. An obligation management report, on the basis of which the reliability of the actors is assessed, is a prerequisite for registering business service providers and currency exchange services.

Registration in the anti-money laundering register is subject to a fee. Provisions on the size of the fee are laid down in the Government Decree on Fees for Regional State Administrative Agencies.

Registration will not be subject to administrative costs in addition to the one-off registration fee. In addition, no fee will be charged for changes to the register data, except for changes in the register data concerning responsible persons for a business service operator or currency exchange service.

If the registered party no longer carries out activities subject to the registration obligation, they must notify the Regional State Administrative Agency for Southern Finland. After the notification, the operator is removed from the anti-money laundering register.

11 Supervision and administrative sanctions

The Regional State Administrative Agency for Southern Finland supervises compliance with the provisions and regulations given in and on the basis of the Money Laundering Act as regards the parties subject to the reporting obligation listed in chapter 1 of this guideline. Chapters 7 and 8 of the Money Laundering Act lay down the provisions on supervision and administrative sanctions.

The Regional State Administrative Agency has the right to obtain, without being hindered by any secrecy provisions and for free of charge, the information and statements it requests that are necessary for carrying out its supervisory duties on the basis of the provisions or regulations given in or on the basis of the Money Laundering Act. The Regional State Administrative Agency may also conduct inspections at the place of business of the party subject to the reporting obligation.

On the basis of the Money Laundering Act, the Regional State Administrative Agency may utilise various methods to intervene in the activities of a party subject to the reporting obligation if any deficiencies are detected in its compliance with the provisions given in or on the basis of the Money Laundering Act.

The Regional State Administrative Agency may issue a prohibition or demand for correction to intervene in any decisions, measures or procedures that the party subject to the reporting obligation has planned or carried out, if these are found to be in violation of the obligations presented in the Money Laundering Act. As a last resort, the Agency may also prohibit a person from serving in the upper management of the party subject to the reporting obligation for a set period of time.

The party subject to the reporting obligation can be issued an administrative fine if it either intentionally or through negligence fails to comply with or violates the obligation to:

1) customer due diligence or to detect and evaluate the risks of money laundering and terrorist financing

2) identify their customers and verify their identity

3) retain its customer due diligence data

4) obtain information concerning a customer, monitor the customer relationship on an ongoing basis and investigate any unusual transactions made by the customer

5) identify the beneficial owner

6) apply the enhanced customer due diligence procedure

7) identify the customer when the customer is not present at the time they are being identified and their identity is being verified

8) create and comply with risk-based procedures to evaluate whether a customer is a politically exposed person, the family member of a politically exposed person, or an associate of a politically exposed person

9) apply the enhanced customer due diligence procedure that is related to high-risk states outside the EEA

10) submit a report concerning a suspicious transaction to the Financial Intelligence Unit

11) apply for inclusion in the anti-money laundering register

12) create the operating methods for reporting suspected violations

13) arrange for the training or protection of its employees or create the operating instructions.

If the aforementioned obligations (excluding the obligation to apply for the anti-money laundering register) are violated or neglected either intentionally or through negligence in a serious, recurring and systematic manner, the Regional State Administrative Agency can issue a penalty payment that, as a rule, is higher than an administrative fine. The Regional State Administrative Agency can also issue a public warning to the party subject to the reporting obligation if it acts in a manner that is contrary to the provisions concerning administrative fines and penalty payments presented in the Money Laundering Act, or in a manner that is contrary to the provisions issued on the basis of the Money Laundering Act. All of the decisions concerning administrative sanctions that are given on the basis of the Money Laundering Act are published on the Regional State Administrative Agency website.

12 Sector-specific instructions

These sector-specific instructions are intended to supplement the Regional State Administrative Agency's guideline on preventing money laundering and terrorist financing. The purpose of the sector-specific instructions is to provide more detailed information and examples of situations in which the Money Laundering Act is applied to parties subject to the reporting obligation in different sectors.

The actual obligations under the Money Laundering Act and the instructions for compliance with these are presented above in the general instructions, and they apply to every sector and every party subject to the reporting obligation.

12.1 Providers of legal services

Providers of legal services as parties subject to the reporting obligation

Pursuant to chapter 1, section 2, subsection 1, paragraph 13 of the Money Laundering Act, the Money Laundering Act applies to a parties who provide legal services as business or professional activities to the extent that legal services act on behalf of and for the customer in transactions related to financial activities or real estate or participate on behalf of the client in the planning or execution of the following transactions:

- buying or selling real property or business entities
- the management of the customer's cash and cash equivalents, securities or other assets
- opening or managing bank, savings or book-entry accounts
- organisation of contributions for the creation, operation or management of companies or
- the establishment management or responsibility for the operations of foundations, companies or similar associations.

The Regional State Administrative Agency has received many enquiries on whether certain general transactions for legal service providers fall within the scope of the Money Laundering Act. For example, drawing up a bill of sale has been determined to fall within the scope of application. Family and estate law transactions are also considered to fall within the scope of application when they are carried out on behalf of and for a customer in transactions involving financial activities or real estate.

The Money Laundering Act also applies to public legal aid attorneys, despite the fact that public legal aid attorneys are public officials. The competent supervisor for public legal aid attorneys is the Regional State Administrative Agency for Southern Finland.

Operators providing legal services are obligated to register in the anti-money laundering register maintained by the Regional State Administrative Agency. The application for inclusion in the anti-money laundering register must be submitted using an electronic form in the Regional State Administrative Agency's e-service.

Risks of money laundering and terrorist financing related to legal service providers

The risks of money laundering related to providers of legal services are often linked to customer relationship monitoring and suspicious customer transactions. In general, there is a risk that the legal service provider is being exploited by a customer to help make their transactions appear legitimate and genuine. For example, the transaction does not have to be illegal in itself, but money that is circulated in the transaction can be the subject of money laundering, and the services of a legal service provider are used with the aim of giving the transaction an official and an amplified legal background.

Customer due diligence

The clients of the providers of legal services constitute customers as referred to in the Money Laundering Act. The contractual relationships of these service providers form a regular customer relationship even though the assignments are typically one-off. This means that customer due diligence measures must be targeted at the contracting partner.

The counterparty of a client of a provider of legal services is not considered to be a customer, in which case the full extent of customer due diligence measures does not need to be extended to them. However, in order to ensure compliance with sanctions legislation, the client's counterparty must be identified at least with sufficient reliability. If necessary, their identity must also be verified. Fulfilment of the obligation to obtain information also often requires acquiring due diligence information on the client's counterparty.

In view of the nature of their activities and their professional skills, legal service providers have special prerequisites for the detection of unusual and suspicious commissions (e.g. fictious business transactions). For this

reason, the importance of measures related to customer due diligence is also emphasised. A basic customer due diligence procedure can be considered a premise for legal service providers. However, an individual customer or commission may involve aspects that warrant a simplified or enhanced procedure. The assessment of the procedure to be used is always based on the company's own risk-based assessment and the Money Laundering Act.

12.2 Financial service providers

Financial service providers as parties subject to the reporting obligation

Under chapter 1, section 2, subsection 1, paragraph 14 of the Money Laundering Act, the Money Laundering Act applies to companies providing financial services. These include companies providing services referred to in chapter 5, section 1, subsection 1, paragraphs 2-11, 13, and 14 of the Act on Credit Institutions (610/2014) and their branches operating in Finland that are not supervised by the Financial Supervisory Authority.

These services include:

- fund raising other than the acquisition of deposits and other repayable funds from the public, or the issue of covered bonds
- lending, financial activities and other financing arrangements
- financing of consumer credit, mortgage credit and trade transactions and factoring
- financial leasing
- provision of payment services and performance of other payment traffic
- issuing electronic money, related data processing and storage of data on electronic media on behalf of another undertaking
- collection of fees
- currency exchange services
- notarial activities
- guarantee activities
- securities trading and other securities activities

- brokerage of housing shares and equity as well as residential real estate related to housing savings activities.

Operators that offer credit or leasing financing are excluded from the scope of the Money Laundering Act. If the company does not itself grant funding or enter into a financing agreement with the customer, and only acts as a platform for comparing different financial products, the activity does not meet the definition of the provision of a financial service and thus does not fall within the scope of the Money Laundering Act.

A company providing an invoicing service shall be considered a financial service provider if the invoicing service includes a credit/financial element and the associated credit loss risk to the service provider.

The Money Laundering Act also applies to the Finnish branch of a company providing financial services that operates in another EEA country.

These sector-specific guidelines apply to companies providing different types of financing. A sectoral annex has been drawn up for currency changers within the definition of financial service providers due to its specificities.

Anti-money laundering register

As a rule, companies providing financial services must apply for inclusion in the anti-money laundering register. It should be noted that, although the definition of companies providing financial services includes the collection of fees, debt collectors must register in the register of debt collection agencies maintained by the Regional State Administrative Agency instead of the anti-money laundering register.

A company providing factoring is considered a company providing financial services and obliged to apply for inclusion in the anti-money laundering register, as is the case with other companies providing financial services. If, on the other hand, a company buys an invoice for itself, the situation is more open to interpretation. In the case of an undue claim transferred to a new creditor, it becomes decisive whether there are other grounds for the transfer of the claim than that the claim may be recovered by a new creditor. If the sales receivables have been purchased exclusively for recovery purposes, the company is regarded as a debt collection agency and it must register in the register of debt collection agencies maintained by the Regional State Administrative Agency. Such an actor does not have to register with the anti-money laundering register. However, the situation is different if a transaction is based on the provision of financing and only a small share of the financed sales receivables ends up in recovery. In this instance, it is not a case of debt collection; instead, it is considered to be provision of a

financial service, and the operator must register in the anti-money laundering register.

The application for inclusion in the anti-money laundering register must be submitted using the electronic form in the Regional State Administrative Agency's e-service.

Risks of money laundering and terrorist financing related to financial service providers

The use of cash, transfers of funds or payment gateways may be classified as significant money laundering risks due to the ease, certainty and speed of the operations, and these transactions do not require any prior planning or expertise. In principle, the risk of money laundering is high for products and services that enable the transfer of funds from one place to another or from one person to another in near real time. On one hand, the provision of financial services has largely gone online, which has contributed to increasing the risks of money laundering and terrorist financing for financial services when transactions and customer identification take place remotely in their entirety.

12.3 Currency exchange services

Currency exchange companies as parties subject to the reporting obligation

Under chapter 1, section 2, subsection 1, paragraph 14 of the Money Laundering Act, the Money Laundering Act applies to companies providing financial services. Under the Money Laundering Act, a company providing financial services refers to a company that carries out one or more of the activities referred to in chapter 5, section 1, subsection 1, paragraphs 2-11, 13 and 14 of the Act on Credit Institutions, as well as to a branch of a company providing financial services located in Finland. Exchange of currency is listed in chapter 5, section 1, subsection 1, paragraph 8 of the Act on Credit Institutions.

Currency exchange companies are obliged to register in the anti-money laundering register kept by the Regional State Administrative Agency. The registration process for currency exchange companies includes a reliability assessment on their responsible persons. The application for inclusion in the anti-money laundering register must be submitted using the electronic form in the Regional State Administrative Agency's e-service.

Risks of money laundering and terrorist financing related to currency exchanges

As a rule, currency exchange can be considered a risky sector for money laundering and terrorist financing. A business involving the abundant use of cash always involves a significant money laundering risk. Transactions at currency exchange points usually consist only of one-off transactions, which makes monitoring the customer relationship more difficult. The use of cash enables the conversion of funds acquired through crime easily and quickly, while the origin and identity of the funds are mostly kept secret.

Customer relationship monitoring and suspicious transactions

The monitoring of a customer relationship in the long term is often impossible for currency exchanges, as these tend to be one-off transactions or some customers must exchange currency occasionally. In these situations, the monitoring of the customer relationship cannot be organised in the same manner as in the case of a regular customer, but even in the case of occasional customers, the currency exchanger is obliged to carry out the identification measures described above and to draw attention to suspicious transactions that may indicate money laundering or terrorist financing, the structure or size of which, or the size or location of the party subject to the reporting obligation, are differ from the norm.

12.4 Operators that provide ancillary services related to investment services

Investment service providers as parties subject to the reporting obligation

Pursuant to chapter 1, section 2, subsection 1, paragraph 16 of the Money Laundering Act, the Money Laundering Act applies to companies providing services referred to in chapter 2, section 3, subsection 1, paragraphs 1-8 of the Act on Investment Services (747/2012). These services include:

- provision of credit and financing related to an investment service
- advice on capital structures, business strategy, business acquisitions, business mergers and other business arrangements
- currency services related to investment services

- the production and dissemination of investment studies, financial analyses and other similar recommendations relating to trade in financial instruments
- a service that guarantees the issuing of financial instruments
- the provision of investment services through underlying derivative contracts that are not financial instruments
- the maintenance and management of financial instruments on behalf of the customer.

The Regional State Administrative Agency supervises compliance with the obligations laid down in the Money Laundering Act for the aforementioned actors that are not supervised by the Financial Supervisory Authority.

Operators providing business consulting and ancillary services related to investment services are obligated to register in the anti-money laundering register maintained by the Regional State Administrative Agency. The application for inclusion in the anti-money laundering register must be submitted using the electronic form in the Regional State Administrative Agency's e-service.

12.5 Pawnbrokers

Pawnbrokers as parties subject to the reporting obligation

Pursuant to chapter 1, section 2, subsection 1, paragraph 17 of the Money Laundering Act, the Money Laundering Act is applied to the pawnbrokers referred to in the Pawnshops Act (1353/1992). A pawnbroker is a limited liability company established for the purpose of pawnbroking and has received authorisation to start operations from the Regional State Administrative Agency. Pawnbroking refers to the provision of financial loans as the main business to natural persons against a movable pawn. In addition to the provision of financial loans, a pawnbroker may sell pawned items if the items are not redeemed by the maturity date of the loan. The pawnbroker must sell the pawned item in a public auction where the pawnbroker can also buy the pawned item and sell the goods so acquired.

Pawnbrokers are listed in a separate licence list, and pawnbrokers do not therefore need to apply for inclusion in the anti-money laundering register.

Risks of money laundering and terrorist financing related to pawnbrokers

Examples of risk factors related to pawnbroker activities include challenges in determining the ownership or origin of the property being pawned and one-off customer relationships. Also, the use of cash increases the risk of money laundering related to business transactions. The use of cash enables the conversion of funds acquired through crime easily and quickly, while the origin and identity of the funds are mostly kept secret. Cash can be moved through informal money brokering channels and cash intensive business into legal circulation.

Customer identification and verification of the customer's identity

A pawnbroker's customer relationship is established when a loan agreement is concluded with the customer. The customer must be identified and their identity must be verified also in connection with the redemption of a pawned item.

The buyer of an unredeemed pawned item is also treated as a customer of a pawnbroker, which is why the buyer must be identified and their identity verified.

Customer relationship monitoring and suspicious transactions

For pawnbrokers, longer-term monitoring of customer relationships is possible if the customers visit the pawnbroker regularly and the information on the pawning transactions is stored appropriately in a customer system. When the pawnbroker is aware of the typical behaviour of its customer, it can detect when their behaviour is exceptional and suspicious.

The monitoring of one-off or first-time customers visiting a pawnbroker is more challenging. However, even for such customers, the pawnbroker is obliged to pay attention to suspicious transactions that are unusual in terms of structure or size, or if the transactions are unusual for the size or location of the party subject to the reporting obligation. The same also applies if the transactions have no apparent economic purpose or if they are inconsistent with the knowledge or experience the party subject to the reporting obligation has of their customer. The detection of suspicious transactions is mainly based on the pawnbroker's professional skills and experience in the field.

A pawnbroker must have adequate procedures to reduce and effectively manage the risks of money laundering and terrorist financing. This means that a pawnbroker must, for example, have instructions on how and in what situations the origin of funds is determined.

Receiving an item to be pawned is one situation where suspicion may arise at a pawnbroker. The pawnbroker must determine the customer's

ownership of the object or property to be pawned in order to fulfil the reporting obligation laid down in the Money Laundering Act.

When the pawnbroker acquires information on the origin or source of the funds in accordance with the Money Laundering Act, a receipt of purchase a register extract, a carry permit, a share certificate, a certificate from a property manager and information from public registers is enough to determine the right of the customer to the item or property to be pawned. The list is not exhaustive. Attention should be paid to the adequacy and reliability of the information. The information on the origin of the funds and the information obtained to fulfil the obligation to obtain information must be retained.

If a pawnbroker is unable to fulfil the obligations laid down in customer due diligence, the customer relationship may not be initiated or the transaction carried out.

12.6 Real estate and rental accommodation brokers

Letting agencies as parties subject to the reporting obligation

According to chapter 1, section 2, subsection 1, paragraph 18 of the Money Laundering Act, the Money Laundering Act applies to real estate agencies and letting agencies referred to in the Act on Real Estate Brokerage and Letting Agencies (1075/2000). Only a private trader or a legal person registered as a broker in accordance with the Act on Real Estate Brokerage and Letting Agencies may carry out letting services. Letting agencies are subject to the reporting obligation under the Money Laundering Act. There are a wide range of actors in the brokerage and letting sector, and, therefore, the risks associated with money laundering and terrorist financing that may vary greatly depending on the sector or extent of the business.

There is a separate register of the Regional State Administrative Agency for real estate and rental accommodation brokers: the register of real estate and lettings agents. For this reason, real estate and rental accommodation brokers are not required to apply for inclusion in the anti-money laundering register.

Customer and identification

As a rule, a customer of a party subject to the reporting obligation under the Money Laundering Act is a client or contracting partner to whom the party subject to the reporting obligation offers goods or services. Real estate brokers are an exception to this rule, and their customers have been

commonly considered to be both the buyers and the sellers, regardless of which party has commissioned them. Thus, the customers of real estate and rental apartment brokers include not only the clients but also the clients' counterparties participating in the transaction commissioned from the broker.

However, the exception rule only applies to the execution of commissioned brokerage. If a real estate broker provides an ancillary service, such as only drawing up the bill of sale, it is a legal service referred to in the Money Laundering Act. In this case, the principal rule is that the client is considered to be a customer.

Providers of legal services (including real estate brokers in the case of an assignment that is regarded as a legal service) must only target customer due diligence measures on their own contracting partner. The client's counterparty is not considered a customer, in which case the due diligence measures referred to in the Money Laundering Act do not need to be extended to them in their entirety. However, in order to ensure compliance with sanctions legislation, the client's counterparty must be identified with sufficient reliability. Fulfilment of the obligation to obtain information also often requires acquiring some information on the client's counterparty as well. However, this only concerns situations where the customer has a counterparty.

If a document such as a bill of sale or lease template is ordered as an open-ended document for later use without entering the details of the other party on it, the service provider cannot be held responsible for the party with whom the customer uses the template later. In such cases when the commission is completed the customer does not have a counterparty that should be identified by the party subject to the reporting obligation on the basis of sanctions legislation or the obligation to obtain information. However, if the party subject to the reporting obligation suspects that the purpose of such a commission is to, for some reason, conceal the identity of the customer's counterparty (that is already known by the customer) from the party subject to the reporting obligation, clarification should be sought of the transaction and, if necessary, a suspicious transaction should be reported to the Financial Intelligence Unit.

The customer, their representative and the beneficial owner must be identified. Identification must be carried out separately for each customer before establishing a customer relationship or conducting a transaction. In real estate transactions, this means that the client must be identified at the time a commission is awarded and the counterparty at the time they submit an offer, but at the latest when the offer has been accepted. The party making an offer must be identified if he or she pays the deposit even if the offer is not accepted.

12.7 Collection agencies

Collection agencies as parties subject to the reporting obligation

Under chapter 1, section 2, subsection 1, paragraph 20 of the Money Laundering Act, the Money Laundering Act applies to the debt collection service operator referred to in the Act on the Registration of Debt Collectors (411/2018) (hereinafter referred to as debt collection act).

Debt collection activities refer to the recovery of receivables on behalf of another party and the recovery of one's own claims in cases where it is obvious that the claims have been received solely for recovery purposes. The Government proposal on the Debt Collection Act (HE 206/2017) states that when the claims have been transferred after their due date these are claims received for recovery purposes. In the case of an undue claim transferred to a new creditor, it is decisive whether there are other grounds for the transfer of the claim than that the claim may be recovered by a new creditor. For example, the transfer of an invoicing claim from the creditor to the financier in factoring activities is not solely a transfer of claims for recovery purposes.

Only a private entrepreneur or a legal person registered as a debt collection operator in a debt collection register maintained by the Regional State Administrative Agency may carry out debt collection activities.

Recovery does not require registration in the Regional State Administrative Agency’s recovery register when:

- the creditor collects his/her own outstanding debts
- the creditor is collecting the claims of an entity belonging to the same group and the debtor is controlled by the same natural person
- the action is enforcement or recovery of claims in a court
- debt collection is occasional and not marketed
- a shareholder in an estate or an estate administrator inherits the claims of the estate or the administrator of a bankrupt estate inherits the claims of the estate
- the supervision of the activities has been arranged by other means, such as credit institutions, funds and insurance companies or other parties supervised by the Financial Supervisory Authority as well as lawyers.

As collection agencies must register in the Regional State Administrative Agency's debt collection register, it is not necessary for them to apply for inclusion in the anti-money laundering register.

Risks of money laundering and terrorist financing related to collection agencies

Money laundering risks related to the debt collection sector may include, for example, participation in international debt collection related to business operations, and individual and large debt collection claims. Individual instant collection commissions make monitoring customer transactions challenging. Unclear and complex claims or payment arrangements may also indicate, for example, a fake debt relationship or an unjustified invoice.

The automation of collection operations and large customer flows can become risks for monitoring the customer's operations, unless the processes have been well implemented. In addition, returns from the customer reserve account related to overpayments and cancelled transactions are subject to a risk. According to the Regional State Administrative Agency's report (2020), collection agencies had some 36,000 unallocated payments, and their total sum at the time the report was submitted was approximately EUR 3.2 million.[1]

Some collection agencies make an effort to contact the debtor to refund their overpayment when the debtor's bank contact details are not known. However, this seemingly sensible approach may end up being a money laundering risk if the debtor gives the account number of another person. Since the collection agency cannot verify the owner of the account, the refund may go to an account other than the debtor's account. Where the collection agency is unable to reach the debtor in order to repay the overpayment and the debtor's account number is not known to collection agency, the return of the overpayment by means of a payment order is a safe way to make sure the refund goes to the correct person.

The procedure used by some collection agencies to prioritise payments in higher amounts and to take more extensive and frequent measures with regard to these may be problematic. The debtor can make payments to the customer reserve account in several instalments. An individual amount does not necessarily evoke interest in reviewing the origin of the funds, but several payments together may constitute a significant amount, the origin of which should be determined. Thus, collection agencies must pay attention

[1] Regional State Administrative Agency supervision letter 21 February 2020: The processing of overpayments and unallocated payments at collection agencies.

to situations where the debtor pays funds in several instalments and the sum of these amounts becomes significant.

The near non-existent use of cash and a permanent customer relationship between the creditor and customer are factors that reduce the risk of money laundering in the debt collection sector. These also make it easier to monitor transactions.

Customer due diligence

The premise for a collection agency's operations can be a basic customer due diligence procedure. However, an individual customer or commission may involve aspects that warrant the collection agency to use the enhanced customer due diligence procedure.

From the perspective of money laundering legislation, the customer of the collection agency is the creditor. The party commissioning a collection procedure must be identified and their identity verified when establishing a customer relationship.

In certain special situations, the party subject to the reporting obligation does not have a customer relationship with an operator referred to in the Money Laundering Act, even though it is a party to the business transactions. An example of this is the debtor from whom the collection agency receives payments based on the customer's assignment. The debtor must always be identified if the transaction appears suspicious or the party subject to the reporting obligation suspects that the assets involved in the transactions are linked to the financing of terrorism.

The collection agency must comply with due diligence in accordance with good recovery practices and ensure that key issues concerning the commission also to the extent that they apply to the debtor. The collection agency relies to a large extent on the information that the commissioning party has provided to the collection agency and for this reason, when receiving a collection assignment, the collection agency must ensure that it has access to the most accurate and up-to-date information possible on the debtor. If the information is incomplete, the collection agency must obtain sufficient information either from the debtor itself, the customer or, for example, from a credit data service or official registers. The Government proposal is not absolute in this matter, which means that there could also be another reliable way of determining identity. The collection agency must determine at least the name and contact details of the debtor.

The Regional State Administrative Agency has changed its previous interpretation of situations where a collection agency purchases a receivables portfolio to its own balance sheet. The seller of the receivables portfolio

becomes the customer of the collection agency. In this case, the customer relationship is based on an agreement on the sale and purchase of receivables. The collection agency must identify the seller of the receivables portfolio and verify their identity. The relationship between a debtor and a collection agency cannot be considered a customer relationship within the meaning of the Money Laundering Act. The debtor is not procuring a service from the collection agency, and the debtor also cannot influence which party carries out the debt collection. Customer due diligence does not need to be extended to the debtor in its entirety. However, in order to ensure compliance with sanctions legislation, the debtor must be identified at least with sufficient reliability. If necessary, their identity must also be verified. Verification could for example be considered in a situation where the authenticity of the due diligence information of the debtor is uncertain. Fulfilment of the obligation to obtain information also often requires acquiring due diligence information on the debtor.

12.8 Business service providers

Business service providers as parties subject to the reporting obligation

Under chapter 1, section 2, subsection 1, paragraph 21 of the Money Laundering Act, the Money Laundering Act applies to companies providing business services. Business service provider refers to an entity or a trader that provides, one of the following services as a business activity to a third party:

- Founding a company on behalf of someone else. As such, selling and buying established businesses is not considered to be business services.
- Acting as a person responsible for company law, a partner or in a similar position in another legal person on behalf of a third party.
- The provision of a domicile, business address, postal address or other similar services.
- Acting as a trustee of an express trust or a similar legal arrangement in Finland.
- Acting as a nominee entered into a shareholder register of a limited company other than a publicly listed company.

Business service providers are obliged to register in the anti-money laundering register kept by the Regional State Administrative Agency. The registration process for a business service provider includes a reliability assessment on their responsible persons, so the registration fee is higher.

In connection with property manager services, it is fairly common that the postal address and/or administrative address of the party receiving property manager services is reported as the address of the operator providing the property manager service. In practice, this can mean that the address recorded in the trade register for a limited liability housing company receiving property manager services is the address of the operator providing the property manager services. In this situation, the operator providing the property manager services should apply for inclusion in the anti-money laundering register as a business service provider. The application for inclusion in the anti-money laundering register must be submitted using the electronic form in the Regional State Administrative Agency's e-service.

Risks of money laundering and terrorist financing related to business service providers

The customer may, for example, seek to set up shell companies with the aim of making the company structures more complex and cover up the identity of its beneficial owners.

As business service providers differ quite a bit from one another, their risks related to money laundering and terrorist financing may vary greatly. Business service providers can be involved in activities such as the formation and management of companies. However, the most common forms of business service in Finland are the establishment of corporations by commission and the provision of an address service.

12.9 Tax advisors

Tax advisors as parties subject to the reporting obligation

Pursuant to chapter 1, section 2, subsection 1, paragraph 22 of the Money Laundering Act, said Act is applied to parties providing direct or indirect tax advice services or taxation-related support as their primary form of business or their primary profession.

The provision of tax advice services or taxation-related support as the primary form of business means that tax advice services or taxation-related support make up at least 50% of a company's operations. Operators that only provide tax advice services on a part-time basis do not fall within the scope of the Money Laundering Act, unless they also provide some other service under the Money Laundering Act and thereby fall within the scope of said Act.

The parties providing tax advice or taxation-related support as their primary form of business are obliged to register in the anti-money laundering register maintained by the Regional State Administrative Agency. The application for inclusion in the anti-money laundering register must be submitted using the electronic form in the Regional State Administrative Agency's e-service.

Risks of money laundering and terrorist financing related to tax advice services

Tax advice services are often related to matters such as national or international corporate acquisitions, generational change situations or questions of inheritance law. Risks in the sector may relate to complex corporate restructuring, complicated transactions and so on. In complex corporate restructuring, identifying the beneficial owners may be difficult. Various actors may also try to use tax advice service providers to disguise or change the origin of funds.

For tax advice service providers, one way to reduce risk is by parties subject to the reporting obligation identifying suspicious requests for advice and carrying out customer due diligence. However, the high threshold for reporting suspicious transactions to the Financial Intelligence Unit has been identified as a risk.

It must also be noted that tax advice services are expert services where the concept of a regular customer also refers to a customer who has only one commission agreement or other commitment with the party subject to the reporting obligation. Due diligence must also be extended to these kinds of customers who only perform a one-off transaction with a party subject to the reporting obligation.

12.10 Accountants

Accountants as parties subject to the reporting obligation

Under chapter 1, section 2, subsection 1, paragraph 23 of the Money Laundering Act, the Money Laundering Act applies to companies that provide accounting services as business or professional activities. On the other hand, the Money Laundering Act does not apply, for example, to persons employed by a company subject to the obligation to keep accounts who handle accounting services.

The reporting obligation of accountants is mainly based on the fact that those working in the sector have the professional skills to identify exceptional and suspicious business transactions.

As a rule, the Money Laundering Act applies to anyone who offers external accounting as a business or professional activity. The Money Laundering Act also applies to an accountant who only carries out some of the tasks related to the accounting areas, such as payroll accounting, but does not offer the so-called "whole package" of accounting services. Even if a tradename entrepreneur is only responsible for the accounting of some companies or housing companies, or the turnover of the accounting firm for the whole year is minor, the Money Laundering Act will apply.

In cases where the Money Laundering Act is not applied to an accountant, the activities are not usually accounting offered as a business or professional activity within the meaning of the Act. The Money Laundering Act does not apply to a layman who manages, for example, the accounts of a housing company in which their housing share is located. Nor does the Money Laundering Act apply to services that do not involve actual accounting management, but rather consulting. If the service provider’s role is mainly to guide and advise other companies in how to manage accounting, this is not a service equal to the accounting referred to in the Money Laundering Act. Also situations where a company manages the accounts of other companies belonging to the same group and does not carry out other accounting for external customers on assignment are not within the scope of the Act.

Accountants are obliged to apply for inclusion in the anti-money laundering register. However, subcontractors who invoice under their own business ID do not need to apply for inclusion in the register if a commission is carried out on behalf of the "parent company" and the subcontractor does not have its own customers.

If the accountant offers several of the services referred to in the Money Laundering Act, all services must be reported in the application. For example, an accounting firm that, in addition to accounting, provides the customer with an administrative address for the trade register must apply for inclusion in the anti-money laundering register as a part-time business service provider.

If the accountant also provides business services, the registration process also includes an obligation management report. In connection with property manager services, it is fairly common that the postal address and/or administrative address of the party receiving property manager services is reported as the address of the operator providing the property manager service. In practice, this for example means that the address recorded in

the trade register for a limited liability housing company receiving property manager services is the address of the operator providing the property manager services. In this situation, the operator providing the property manager service should apply for inclusion in the anti-money laundering register even as a business service provider.

Risk assessment

An accountant must prepare a written risk assessment suitable for their own activities. As the accountants' reporting obligation is primarily based on the accountants' ability to detect suspicious transactions carried out by accounting clients, the accountant's risk assessment differs slightly from the risk assessment of other parties subject to the reporting obligation.

The majority of parties subject to the reporting obligation fall within the scope of the Money Laundering Act because they can be taken advantage of for money laundering or terrorist financing. These parties subject to the reporting obligation must assess the risks related to their own sector in their own risk assessment. On the other hand, the accountant's risk assessment does not focus solely on the financial administration sector, as accountants mainly assess the risk factors related to their own customer base and their customers' sectors.

In order to determine the sufficient extent and coverage of the risk assessment, those offering accounting services must take into account the nature, size and extent of their activities. In addition, in their risk assessment, the accountant must examine, among other things, the sector and the nature, size and extent of the activities of accounting customers. Particular attention must therefore be paid to assessing customer-related risks. A deficiency that is typically discovered in accountants' risk assessments is that the risks associated with the customer base and the activities carried out by the customers have not been sufficiently assessed.

Customer due diligence

According to the Money Laundering Act, the party subject to the reporting obligation must identify their customer and verify their identity when establishing a regular customer relationship. A customer relationship is considered regular when the accountant concludes an agreement for the management of the customer's accounts.

The obligation to identify the customer and verify their identity applies to both new and old customers. These obligations must also be fulfilled when

the accountant personally knows the customer or their representative, for example due to them being a close friend or relative.

Accountants typically have very long-term customer relationships. This means that accountants must pay attention to updating their customer information regularly. Accountants must have a clear operating model for ensuring that their customer information for long-term customers is continuously up to date.

Customer relationship monitoring and suspicious transactions

Due to their professional skills and job description, accountants are able to monitor the customer's activities. An accountant has access to the customer's accounting records and is well aware of the customer's financial situation.

If the accountant observes a suspicious transaction, they must try to obtain additional information about it. For example, an accountant may request to see the original contracts concluded by the accounting customer on which the suspicious transaction is based. If, even in the light of the additional information obtained, the transaction appears suspicious or proper information showing otherwise cannot be obtained, the accountant must submit a report of the suspicious transaction to the FIU without delay. For example, if an accountant suspects tax evasion, VAT fraud or the practice of activities within the scope of the shadow economy these must be reported to the Financial Intelligence Unit.

12.11 Goods dealers

Goods dealers as parties subject to the reporting obligations

Under chapter 1, section 2, subsection 1, paragraph 24 of the Money Laundering Act, the Money Laundering Act applies to those selling or supplying goods by way of business or profession to the extent that a payment is made or received in cash totalling EUR 10,000 or more, whether the transaction is executed in a single operation or in several operations which are linked. Cash refers to physical banknotes or coins. Debit card payments or credit transfers from a bank account are excluded from the definition of cash in the Money Laundering Act.

The government proposal on the Money Laundering Act (HE 228/2016 VP) states that traders may in some respects refuse to receive cash if the refusal meets the conditions laid down in the Commission Recommendation on the scope and effects of legal tender of euro banknotes and coins

(2010/191/EU). The trader must clearly inform about this, for example outside their shop. The acceptance of cash payments totalling EUR 10,000 or more may be refused, for example, on the grounds that the receipt of large amounts of cash constitutes a risk of being targeted in a criminal offence. The risk could be caused, among other things, by the geographical location of the business premises. According to the Bank of Finland's policy on cash services, based on the contractual freedom prevailing in Finland, a shop can choose the payment methods it accepts, provided that it clearly informs customers of this before they make their purchase decisions. In addition, the guideline[2] issued by the Finnish Competition and Consumer Authority concerning cash states that the Act does not contain a provision that would oblige traders to accept cash as a form of payment. Even so, it should be noted that the consumer must be separately informed at the marketing stage if cash is not an accepted form of payment in the store, so that consumers can take this into account when choosing the place of purchase.

The concept of 'goods' and the whole group of goods is quite extensive and nothing specific can be excluded from its scope in advance. The European Union[3] has also found that the concept of goods is as broad as the range of existing goods, provided that the goods have economic value. All operators selling or brokering goods that receive cash payments exceeding or totalling EUR 10 000 are within the scope of application of the Money Laundering Act. However, the sale of goods must be separated from the sale of services, which is not in the scope of the Money Laundering Act's provisions concerning trade in goods.

With regard to the application of the law, it is irrelevant how often cash payments exceeding the threshold occur in the trader's business. Goods dealers are included in the scope of application of the Money Laundering Act as soon as they first receive an individual cash payment or a series of linked cash payments of EUR 10,000 or more.

An actor must apply for inclusion in the anti-money laundering register when a company or a private trader first receives an individual payment or linked payments totalling EUR 10,000 or more. The application for inclusion in the anti-money laundering register must be submitted using the electronic form in the Regional State Administrative Agency's e-service.

[2] https://www.kkv.fi/Tietoa-ja-ohjeita/Maksut-laskut-perinta/laskutustavat/#kateinen

[3] European Commission: Guide to the application of Treaty provisions governing the free movement of goods (2010), p. 9, and the EU court's ruling practice.

Risks of money laundering and terrorist financing related to the trade of goods

The use of cash increases the risk of money laundering related to business transactions. The use of cash enables the conversion of funds acquired through crime easily and quickly, while the origin and identity of the funds are mostly kept secret.

There are very different types of goods dealers within the trade of goods sector, and the risks related to money laundering and terrorist financing may vary greatly. The ability of different parties subject to the reporting obligation to notice unusual transactions will depend on the sector and scope of their activities. Actors within the trade of goods sector include vehicle dealers, construction equipment dealers, household appliances shops, watch and jewellery shops, fur shops and shops that sell various valuables, to the extent that they receive cash payments totalling at least 10 000. The list is not exhaustive.

Customer identification and verification of the customer's identity

Dealers of goods must identify their customer and the customer’s representative and verify their identity in situations falling within the scope of the Money Laundering Act, i.e. when selling or brokering goods when payments are made in cash or received as cash in the form of a single payment or a series of linked payments totalling at least EUR 10,000. Also, when the customer has, for example, a purchase account at the shop, but they make a payment of 10,000 euros or more in cash exceptionally, the identification and verification measures laid down in the Money Laundering Act must be carried out.

The customer must be identified, and their identity verified both in the case of individual cash payments totalling or exceeding EUR 10,000 and in the case of linked cash payments totalling at least EUR 10,000. Identification must be carried out when the said limit is reached. There is no definitive explanation on what is meant by linked payments. However, this has been used with the aim of preventing situations where a customer could try to avoid verifying their identity by dividing the funds included in the transaction into several separate payments. Identification and verification measures must be carried out, for example, when a private person purchases a vehicle that costs EUR 10 000 and pays in cash. Situations where payments may be linked can include those where the customer buys, for example, a necklace for EUR 5,000 and soon returns to the same store to buy a watch costing EUR 5,000.

Customer relationship monitoring and suspicious transactions

In the case of goods dealers, the longer-term monitoring of the customer relationship may be more difficult, for example due to one-off sales transactions or if a customer only occasionally purchases the trader's products. In this case, it may be more difficult to detect activities that are abnormal for the customer in question. However, goods dealers are obliged to carry out customer identification activities and to draw attention to suspicious transactions that may indicate money laundering or terrorist financing, the structure or size of which deviate from the norm, or when the size or location of the party subject to the reporting obligation are different from the norm. As a rule, cash payments exceeding or totalling EUR 10,000 can be considered exceptional these days, as the use of cash as a form of payment has decreased significantly in recent decades. With regard to cash payments exceeding or totalling EUR 10,000, the obligation to obtain information under the Money Laundering Act must be observed with special care and suspicious transactions must be reported at a low threshold to the Financial Intelligence Unit.

12.12 Art dealers

Actors that sell art or act as intermediaries in the sale of art are subject to the reporting obligation

Under chapter 1, section 2, subsection 1, paragraphs 25 and 26 of the Money Laundering Act, the Money Laundering Act applies to the sale or brokering of artworks as a business or professional activity to the extent that cash is paid or received as a payment in the form of a single payment or linked payments totalling EUR 10,000 or more.[4] With regard to the application of the Act, it is irrelevant how often payments exceeding the limit are made in the trader's business transactions, as actors who sell and broker art will be included in the scope of application of the Money Laundering Act the first time they receive an individual payment or a series of payments totalling EUR 10,000 or more. Payments can be made in any form.

Actors selling or brokering art may include art galleries engaged in the sale, purchase and brokering of art as business or professional activities, persons selling art under their trade name or through a company, as well as antique shops and auctioneers selling, buying or brokering art.

[4] The obligations also apply to parties selling, brokering and storing art through a freeport. A freeport is a limited part of a port through which goods are subject to separate customs treatment. There are no freeports in Finland.

Only sales of art works and their related payments which have taken place after 1 December 2019 are within the scope of application of the Money Laundering Act. Consequently, the Act is not applied retroactively and, for example, contracts or projects that have started before the Act entered into force do not fall within the scope of the Act.

The Money Laundering Act is not applied to registered associations whose art mediation services is not a business or professional activity. This could refer, for example, to a non-profit association of general interest with several tasks, one of which is gallery activities and art work brokering. Whether the activities carried out by the association or an equivalent operator are business or professional activities is decided on a case-by-case basis.

The price of an art work determines whether the Money Laundering Act applies to the activities. In a situation where an artist occasionally sells a work worth 10,000 euros from their own art studio and the material costs of the art work were, for example, 8,000 euros, the activities are within the scope of the Money Laundering Act. On the other hand, if, for example, the customer delivers the materials, they are not part of the total (sales) price of the work.

When a commercial gallery handles a customer meeting and payment traffic on behalf of an artist it represents, the gallery is subject to the reporting obligation when brokering works of art. The Finnish Money Laundering Act only applies to activities carried out in Finland, which means that when a gallery is located abroad the legislation of the location country applies.

The scope of application of the Money Laundering Act does not include a public display grant received for the production of public art, an artist's salary in the scope of an employment contract or similar performance in the form of remuneration for work, or a prize received from an art competition. If, in addition to the above, a separate sales price of at least EUR 10,000 is paid for the work, the Money Laundering Act shall apply to the payment.

If an artist produces and sells an artwork to a public body (e.g. the state, a municipality, a hospital district), the money laundering risk can be considered to be lower. An artist is often paid a salary for public art, or the work is paid for according to the percent for at scheme. Public art refers to a work produced in a certain space or for a certain space. It can be a multi-form work and is not intended to be sold forward, so it rarely has an exchange value. Public art differs from the traditional trade of movable artworks, whose money laundering risk relates to the easy mobility of such movable art.

On the basis of a consistent interpretation of the Money Laundering Act, an artist's salary or similar payment in the form of a remuneration for work or

commission agreement obtained for the production of non-public art is also excluded from the scope of the Act.

Anti-money laundering register

Actors that sell or broker art as a business or professional activity are obliged to register in the anti-money laundering register kept by the Regional State Administrative Agency when artworks are sold for at least EUR 10,000 and paid in one or linked payments. The application for inclusion in the anti-money laundering register must be submitted using the electronic form in the Regional State Administrative Agency's e-service.

A company or a private trader must apply for inclusion in the anti-money laundering register when they first receive an individual payment or linked payments totalling EUR 10,000 or more for the sale of an artwork. The application for inclusion in the anti-money laundering register must be submitted using the electronic form in the Regional State Administrative Agency's e-service.

Registration will not be subject to administrative costs in addition to the one-off registration fee. For example, in a situation where an artist sells an artwork worth at least EUR 10,000 to one buyer one year, but does not sell any works in the following years, the artist will remain in the register.

However, if an artist no longer carries out activities subject to the registration obligation, the artist must notify the Regional State Administrative Agency for Southern Finland of this, after which they will be removed from the anti-money laundering register.

What is an artwork?

The artwork referred to in the Act includes both works of art, objects and intangible art. The concept of an artwork or work of art has not been unambiguously defined in any law, but the definition of an artwork used in the Value Added Tax Act can be used in this context to assist in defining an artwork. According to section 79c of the Value Added Tax Act, works of art refer to certain goods classified in the customs tariff as provided for in the VAT Act. Traditionally, prints, paintings, drawings, pastels, graphics, collages, statues, sculptures, glass art, hand-woven images and hand-made wall clothing are considered works of art. Photographic art comprises photographs that have been taken and printed by the artist or numbered, signed and printed in the artist's presence and are limited to 30 copies. In the scope of the law, intangible art, such as lighting art, audio art and an artistic performance, is also considered an artwork. An artwork must be

unique and, in certain situations, no more than eight copies of the artwork can be produced. Copies made through mass production and ordinary handicraft products that are goods by nature are not considered works of art.

Risks of money laundering and terrorist financing related to actors that sell and broker art

The possible use of cash, occasional customer relationships and subjectivity of artistic value may expose actors in the field to risks.

Artworks are sold and brokered by very varied groups of actors from private traders to galleries and auctioneers, and the risks related to money laundering and terrorist financing may vary greatly. The ability of different parties subject to the reporting obligation to notice unusual transactions will depend on the sector and scope of their activities.

Based on observations made under the supervision of the Regional State Administrative Agency, the art market in Finland is limited and known among enthusiasts in the field. The sale and purchase of art mainly takes place through known art galleries and auctioneers. In recent years, art galleries and auctioneers have entered the Finnish market through new technologies. These operate internationally through online commerce, which means that as remote identification increases, the measures related to customer due diligence will be of greater importance. Due to the nature of the activities of the art dealer, the mutual knowledge of the people in the sector and the professional skills of the staff, there are special prerequisites for detecting abnormal and suspicious transactions.

Customer identification and verification of the customer's identity

Dealers that sell or broker art must identify their customer and the customer’s representative and verify their identity in situations falling within the scope of the Money Laundering Act, i.e. when selling or brokering works of art, when payments are made in cash or received as a single payment or a series of linked payments totalling at least EUR 10,000. The identification obligation must be fulfilled separately for each customer and it must be carried out before establishing a customer relationship or conducting a transaction. Also, in situations where a customer is already familiar to the party subject to the reporting obligation and they have a purchase account in an art shop, but the customer exceptionally makes a payment of total or more than EUR 10,000, the identification and verification measures laid down in the Money Laundering Act must be carried out.

The customer must be identified and their identity verified both in the case of individual payments totalling EUR 10,000 or more and in the case of linked payments totalling at least EUR 10,000. Identification must be carried out when the said limit is reached. There is no definitive explanation on what is meant by linked payments. However, this has been used with the aim of preventing situations where a customer could try to avoid verifying their identity by dividing the funds included in the payments into several separate transactions. Identification and verification measures must be carried out, for example, when a private person purchases a work of art that costs at least EUR 10,000 and pays with any form of payment. Situations where payments may be linked can include when a customer buys a work of art for EUR 5,000 and then returns to purchase another work of art for EUR 5,000 from the same party.

With regard to public art, it may be sufficient for the customer to be identified using the simplified due diligence procedure. This means that the customer due diligence procedure can be lighter and no additional documents need to be obtained. The simplified due diligence procedure must be justified with reasons related to the transaction or the customer. Its use must also be justified in the risk assessment prepared by the party subject to the reporting obligation.

Customer relationship monitoring and suspicious transactions

The long-term monitoring of a customer relationship may be more difficult for actors that sell or broker art, if the customer only makes a one-off purchase or only purchases artwork occasionally. However, even in the case of occasional customers the actor selling or brokering art has an obligation to carry out customer identification activities and to draw attention to suspicious transactions that may indicate money laundering or terrorist financing, the structure or size of which deviate from the norm, or when the size or location of the party subject to the reporting obligation are different from the norm. Suspicious transactions should be reported at a low threshold to the NBI’s Financial Intelligence Unit (FIU).

Additional information

Instructions for preparing a risk assessment

Instructions for reporting suspicious transactions

Enforcement of the Anti-Money Laundering Act, website by the Regional State Administrative Agency

Rahanpesu.fi - Prevent money laundering and terrorist financing

Regional State Administrative Agency’s e-service – application form for the anti-money laundering register

Attached documents

This is an example of a customer information form template for parties subject to the reporting obligation. There may be special features and different risks that apply to different sectors and customer relationships. That is why this form template is not suitable as such for every situation or for use by every party subject to the reporting obligation.

Customer information form template

Basic customer information (natural person)	
Name	
Date of birth	
Personal identity code	
Address	
Customer is a PEP (politically exposed person)	Yes ☐ No ☐
Customer is a family member of a PEP	Yes ☐ No ☐
Customer is an associate of a PEP	Yes ☐ No ☐
Confirmed that the customer is not a person on a sanctions list or frozen funds list	☐ Date:
Information used for identity verification	
Document name	
Document number or other identification data	
Issued by	
Copy of document	☐
Met	In person ☐ Remotely ☐
Information on the procedure or sources used for verification (if identified remotely)	
Used strong electronic identification or other, please specify	☐

Basic customer information (legal person)	
Full name of legal person	
Business ID / Registration number	
Registration date	
Registration authority	
Domicile address	
Address of principal place of business, if different from domicile address	
Legal person's field of business	
Copy of Trade Register extract or other similar extract	☐
Articles of association or by-laws attached if necessary	☐
Confirmed that the customer is not an organisation on a sanctions list or frozen funds list	☐
Board of directors of legal person (information of each member)	
Member I	
Full name	
Date of birth	
Nationality	
Representative	
Name	
Date of birth	
Personal identity code	
Right to represent	☐ (Include document ensuring the right to represent)
Information used for identity verification	
Document name	
Document number or other identification data	
Issued by	

Copy of document	☐
Met	In person ☐ Remotely ☐
Information on the procedure or sources used for verification (if identified remotely)	
Used strong electronic identification or other, please specify	☐

Beneficial owners (information of each actual beneficiary)	
I Name of beneficial owner	Date of birth
Personal identity code	Nationality
Position/role in legal person	
Beneficial owner is a PEP (politically exposed person)	Yes ☐ No ☐
Beneficial owner is a family member of a PEP	Yes ☐ No ☐
Beneficial owner is an associate of a PEP	Yes ☐ No ☐
Share of ownership (%) or voting rights in legal person	
Detailed description of ownership and control structure	
Confirmed that the beneficial owner is not a person on a sanctions list or frozen funds list	☐ Date:
Information used for identity verification (if applicable)	
Document name	
Document number or other identification data	
Issued by	
Copy of document	☐

Met	In person ☐ Remotely ☐
Information on the procedure or sources used for verification (if identified remotely)	
Used strong electronic identification or other, please specify	☐
Customer operations	
Description of the customer's operations	
Description of the nature and extent of business	
Description of the grounds for the use of transaction or service	
Are the operations international?	Yes ☐ No ☐
Does the customer have links to a high-risk state?	Yes ☐ Which states? No ☐
Has the customer or the customer's representative been met in person?	Yes ☐ No ☐
Description of the customer's financial position	

Information on the origin of the funds	Yes ☐ No ☐ Clarification:
Has upper management approved the initiation of the customer relationship? (Customers within the scope of enhanced customer due diligence)	Yes ☐ No ☐

Regional State Administrative Agency for Southern Finland