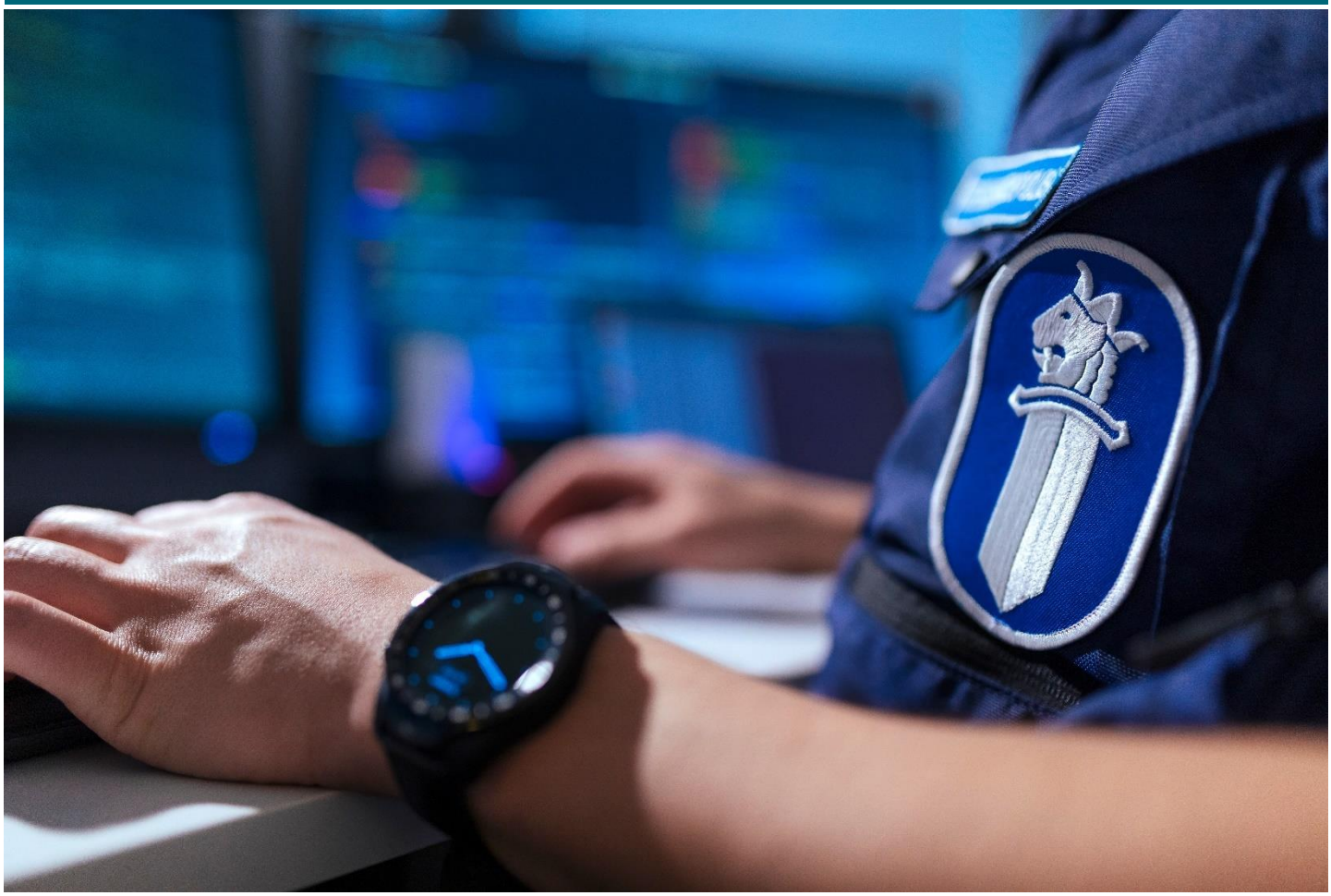
Money Laundering and Terrorist Financing Indicators



National Bureau of Investigation, Financial Intelligence Unit (FIU)

Abstract

REPORT NAME	Money Laundering and Terrorist Financing Indicators
PUBLICATION NAME	Money Laundering and Terrorist Financing Indicators
COMPILED BY	Irene Heikkilä, inspector
TIME OF PUBLICATION	25.4.2023
ASSIGNMENT/RESEARCH QUESTION	Financial Intelligence Unit
MAJOR SOURCES	Major sources are listed on page 43
KEYWORDS	Money laundering, terrorist financing, indicator, money laundering report, obliged entity
PUBLICITY LEVEL	Public

ABSTRACT/MAIN FINDINGS

The Financial Intelligence Unit has compiled a list of money laundering and terrorist financing indicators that obliged entities should monitor in their operations. The purpose of the list is to describe by sector the most common indicators of money laundering and terrorist financing. The objective with the list is to support obliged entities in preventing money laundering. The list of indicators is not exhaustive. On the other hand, meeting the listed criteria does not necessarily mean that an activity involves money laundering or other criminal activities.

The report starts by a review of some of the cornerstones of the prevention of money laundering and terrorist financing, followed by a more detailed analysis of indicators related to terrorist financing and other general indicators. Sector-specific indicators are discussed in more detail starting from Chapter 5. Although this list of indicators is organised by sector, it should be kept in mind that many of the indicators are general and applicable to several sectors, meaning that the report should be considered as a whole.

This list of indicators is an updated version of the Money Laundering Indicators report published in 2021.

PAGES 43

Contents

1 Introduction

The Financial Intelligence Unit has compiled a list of money laundering indicators for the special attention of obliged entities in their operations. The primary purpose of the list is to assist obliged entities to identify suspicious aspects of various activities that could suggest money laundering. The list of indicators is not exhaustive. On the other hand, meeting the listed criteria does not necessarily mean that an activity involves money laundering, terrorist financing or any other criminal activities.

Due to the large number of obliged entities and differences between sectors, the indicators have been listed by sector. Many of them are nevertheless general and applicable to a number of sectors.

Information on the prevention of money laundering and terrorist financing, as well as current news on the subject, are available at www.rahanpesu.fi, a website managed jointly by several parties.

The objectives of the Act on Preventing Money Laundering and Terrorist Financing (444/2017, MLA) are 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.

The obliged entities and their reports of suspicious transactions play a central role in the prevention of money laundering. The cornerstones of combating money laundering are:

- Identifying the customer from a reliable source (verification of identity)
- Performing customer due diligence (nature and scope of business, cash flow, rationale)
- Establishing the source of funds
- Monitoring customer relationships and updating customer information

Obliged entities are not permitted to establish a customer relationship, conduct a transaction or maintain a business relationship if they are not able to implement the anti-money laundering cornerstones.

2 Key considerations on the prevention of money laundering

2.1 Customer due diligence and customer profile

Customer due diligence is one of the most important measures an obliged entity must take to prevent money laundering and terrorist financing. Only by knowing the customer is it possible to create a customer profile. Customer due diligence and a customer profile allow the entity to assess and identify suspicious transactions, which is crucial to the reporting obligation.

Understanding the customer profile is essential when assessing unusual and suspicious transactions, as it is the customer profile that determines whether a transaction is normal or abnormal. The customer profile is based on information provided by the customer and reference information obtained through the obliged entity's own investigations. The customer profile consists of identifying information, financial data, the transaction history and the customer's behaviour. Aspects to consider when reviewing a customer profile include the customer's reported source of income in relation to their actual income and the sector. Identifying aspects that lead to the need to conduct further investigations or obtain reference information can be challenging. As a general rule, any and all uncertainties in a customer relationship should be investigated further. The higher the assessed risk, the more carefully the customer needs to be investigated and profiled.

Customers should be asked to provide any required additional information in writing. Accepting verbal information is not recommended. The obliged entity may demand business documentation such as business certificates, extracts from registers and copies of bills of sale to complete the investigation.

In addition to the information provided by the customer, various types of reference information are used to create the customer profile, including information obtained from public registers and trade register extracts, as well as information on any business prohibitions or a bad credit record. Obliged entities can also use open sources of information to find reference information on customers, their business operations, or the assets and parties involved in their operations.

2.2 Suspicious transactions

An obliged entity must report a suspicious transaction to the Financial Intelligence Unit immediately after having detected the suspicious business transaction or suspected terrorist financing. Suspicious transactions can be identified by comparing them to ordinary business transactions in the sector, the normal behaviour of similar customers or customer groups, or the typical use of specific products or services.

Any unusual activity or activity deviating from the customer's normal operations, including operations with unusual financial value, should be considered suspicious, while also taking into account the customer due diligence results. The nature of a transaction should first and foremost be evaluated in light of general experience of the sector, i.e. what activities should be considered suspicious in any given sector. If a customer acts contrary to the assumptions based on the preliminary information provided by them (the customer due diligence or customer profile) or the customer's operations change without a reasonable explanation, such as a commercial reason, this should raise suspicions about the customer relationship itself.

The suspiciousness of a transaction should first and foremost be evaluated by comparing the transaction to the customer profile or the normal course of business in the sector. This means that a transaction could be in line with one customer's regular business operations, but deviate from the profile of another one, raising suspicions of criminal activity. Sufficient information from the customer is required to know the customer and meet the obligation to request information.

In assessing the money laundering and terrorist financing risks in a customer relationship, an obliged entity must take into account the money laundering and terrorist financing risks relating to its customers and to specific countries or geographic areas, as well as to products, services and transactions (MLA, Chapter 3, section 1, subsection 2).

Obliged entities are not required to assess whether a transaction constitutes a criminal offence – a money laundering report is not a report of an offence. A money laundering report should be submitted without delay to prevent the funds in question from being transferred out of reach of the authorities. Obliged entities should not set their internal reporting thresholds too high, as the responsibility for investigating the source of the funds and the true nature of the transaction lies with the Financial Intelligence Unit. Any criminal offence that generates proceeds can be a predicate offence. For example,

assets obtained by fraud and taxes avoided by committing a tax offence in the course of legitimate business are both considered proceeds of crime.

The following general indicators can be considered to apply to all sectors:

- ✓ A customer does not provide the information requested by virtue of the obligation to request information.
- ✓ The obliged entity considers a customer's report unreliable or doubts the authenticity of documents.
- ✓ The information obtained by the obliged entity does not adequately explain the rationale for a transaction and the source of the funds.
- ✓ The obliged entity is unable to identify or reliably determine the legal entity, beneficial owner or individual on whose behalf a customer is acting.
- ✓ A transaction involves significant amounts of cash.
- ✓ The addresses or contact details of responsible persons are constantly changing.
- ✓ A customer has a connection to a country whose money laundering and terrorist financing prevention system does not meet international standards, and the facts related to the transaction cannot be reliably established.[1]

2.3 Determining the authenticity of identification

An identity theft is most typically committed with a stolen identification document. In such a case, the perpetrator opens a bank account and obtains online banking credentials with a stolen or misplaced identification document. With the credentials, the perpetrator can then commit an offence such as taking out a payday loan using the account just opened, directing the bills to the victim.

Due to the ease of identity theft, bank employees should pay particular attention to identification documents and actually identify the customer based on the photograph.

In Finland, customers are usually identified from a passport, a Finnish driving licence or an ID card with a photo. Attention should be paid to the

[1] Government proposal 228/2016 vp, p. 111

authenticity of the documents. Check the following when determining the authenticity of a document:

1) Is the document intact, or has it been torn or folded, or is its surface damaged? If the document is in poor condition, there is a greater risk that the details have been changed (such as switching the photograph or changing the date of birth).

2) Look at the customer's face and compare it with the photograph on the identification document:

- Concentrate on the essential; focus on the face and try not to let the hair draw your attention.

- Look at the features from top to bottom (eyes, nose, mouth and jaw); look for differences and similarities in comparison to the photograph.

- Pay attention to any distinguishing marks such as moles or scars. Do remember, however, that such marks can change over time.

- Note that the angle of view can have a significant impact on identification.

3) Examine the document's technical properties and security features. Keep in mind that the authenticity of a document is impossible to determine from a photocopy, and verification of the authenticity of a document in retrospect is not possible.

If identification is hindered by a religious scarf, for example, you can ask the customer to rearrange the scarf so that their face can be seen properly. You can also ask the customer to move their hair or remove their glasses if these obstruct their face.

Also follow these three important guidelines for verifying documents:

1) Time; take at least a few minutes to confirm the authenticity of the document.

2) Tools; use at least a loop when comparing documents. Ultraviolet light is also recommended for verifying holograms.

3) Points of reference; compare the document being examined to an original (from online directories), paying special attention to the security features of the identification document.

For assistance in comparing identification documents, we recommend the Public Register of Authentic identity and travel Documents Online (PRADO)

maintained by the Directorate-General for Justice and Home Affairs of the General Secretariat of the Council of the European Union.[2] Another recommended identification/comparison tool is EdisonTD.[3]

2.4 Exceeding the threshold

According to the Act on Preventing Money Laundering and Terrorist Financing (MLA, Chapter 4, section 1, subsection 2), money remittance service providers are obliged to report every payment or remittance that has a value of at least EUR 1,000, whether carried out individually or in a number of linked operations. Other obliged entities may also set reporting thresholds on the basis of their own risk assessments and report payments or transactions that exceed these thresholds. This gives obliged entities the opportunity to take the special characteristics of their operations into account in setting the threshold. For example, it can be difficult for obliged entities with mostly one-time customers to create customer profiles and keep track of connected transactions. A monetary threshold will lower the threshold for reporting especially in cases where identifying individual suspicious transactions is challenging. Setting thresholds is especially recommended for obliged entities whose operations entail a particularly high money laundering risk. The Financial Intelligence Unit can discuss with the obliged entity the effects of a specific threshold on the quality and quantity of reports.

2.5 Confidentiality obligation

An obliged entity must not disclose the submittal of the report to the individual whom the report involves or to any third parties. This confidentiality obligation also applies to employees of the obliged entity and anybody who has received confidential information.

However, notwithstanding the confidentiality obligation, the obliged entity may disclose the fact that a report has been submitted to another obliged entity involved in an individual transaction relating to the same customer and the reported transaction. For the development of obliged entities' operations, the disclosure of information between obliged entities is desirable to the extent permitted by law.

[2] http://www.consilium.europa.eu/prado/fi/prado-start-page.html
[3] http://www.edisontd.net/

2.6 Lists of high-risk countries by the European Commission and FATF

The European Commission and FATF maintain lists of countries that are considered to have significant deficiencies in their anti-money laundering and terrorist financing legislation or measures. According to information available to the Financial Intelligence Unit, Turkey and Somalia are among the high-risk countries for terrorist financing.[4]

High-risk areas in particular from the perspective of terrorist financing have not been separately listed, but may include areas where terrorists operate, areas where terrorists reside and countries from which terrorist activities may be financed.

FATF maintains a blacklist of high-risk countries (High-Risk Jurisdictions subject to a Call for Action)[5]. Countries considered uncooperative in the global effort to combat money laundering and terrorist financing have been blacklisted.

The FATF grey list (Jurisdictions Under Increased Monitoring)[6] includes countries that have a high risk of money laundering and terrorist financing but have formally committed to working with FATF to develop action plans to address the shortcomings in their anti-money laundering and terrorist financing measures.

The European Commission maintains a list of high-risk countries outside the European Economic Area[7]. If an obliged entity conducts transactions or makes payments in relation to non-EEA countries identified by the Commission as high-risk countries for money laundering and terrorist financing, the obliged entity must comply with the enhanced customer due diligence procedures specified in the Act on Preventing Money Laundering and Terrorist Financing.

The obliged entity should pay particular attention and apply enhanced due diligence to customers and transactions with links to countries on the lists of the European Commission and FATF. Enhanced customer due diligence due to geographical risk is provided for in Chapter 3, sections 10 and 13a of the Act on Preventing Money Laundering and Terrorist Financing. Enhanced customer due diligence requires more extensive investigation and documentation of the customer's operations and service use.

[4] Financial Intelligence Unit, Selvitys terrorismin rahoittamisen ominaispiirteistä (poliisi.fi)
[5] Documents - Financial Action Task Force (FATF) (fatf-gafi.org)
[6] Documents - Financial Action Task Force (FATF) (fatf-gafi.org)
[7] High risk third countries and the International context content of anti-money laundering and countering the financing of terrorism (europa.eu)

2.7 European Commission's list of non-cooperative jurisdictions for tax purposes

Suspicious customers and transactions often involve tax havens and related financial institutions, which means that obliged entities should pay particular attention to these. The EU has published a blacklist[8] of countries that do not respect the principles of tax transparency and fairness. The EU also maintains a grey list of countries committed to amending their detrimental tax systems. For more information on tax haven indicators, see Chapter 13.

2.8 International sanctions

International restrictive measures or 'sanctions' refer to restrictions on economic or other cooperation with designated entities aimed at influencing their policies or activities that have been deemed to be a threat to international peace and security. Sanctions can take the form of financial sanctions to combat terrorism or other financial restrictive measures to freeze assets.

Sanctions usually target specific designated individuals and entities considered responsible for the actions or policies opposed by the sanctions or considered to support such actions or policies. Sanctions can also be targeted at the funding sources of such individuals and entities. Assets held by individuals and entities on the sanctions list must be frozen, and any form of commercial activity with them must be refused. The website of the Ministry for Foreign Affairs lists the sanctions imposed on EU member states by country[9]. General information on sanction schemes is available on the sanction website of the Ministry for Foreign Affairs[10].

Finland's national public list of administratively frozen terrorist funds can be ordered from the registry of the National Bureau of Investigation. The list is automatically sent twice a year to obliged entities registered via the reporting channel of the Financial Intelligence Unit. Administrative freezing of funds is regulated by the Act on the Freezing of Funds with a View to Combating Terrorism (325/2013).

If a company notices a party whose details match the identifying information of a sanctions target in its customer registers or payment transactions, it must immediately freeze their assets and terminate any unfinished transactions. The Helsinki Enforcement Agency must also be notified of the matter at helsinki.uo@oikeus.fi. Sanction list hits often also justify a report to the

[8] EU list of non-cooperative jurisdictions for tax purposes - Consilium (europa.eu)
[9] https://um.fi/pakotteet-maittain
[10] https://um.fi/pakotteet

Financial Intelligence Unit. Violations of the obligations related to international sanctions are punishable as a regulation offence under Chapter 46 of the Criminal Code of Finland (39/1889).

3 General indicators

Cash is still commonly used in money laundering and terrorist financing, as it can be used without revealing the offender's identity or the source of the funds, which means that it is nearly impossible to trace.

Cash from illegal sources can be deposited into personal bank accounts, but can also be laundered in legal business operations or through business with the appearance of legality. Lines of business that typically involve large amounts of cash entail a particularly significant money laundering risk according to the European Commission's multinational risk assessment. Such sectors include the restaurant industry, commerce and retail, auctions, the construction industry, the car business and service stations, pawnshops and gambling services. Offenders may try to present criminally obtained cash funds as income obtained from business activities.

Both national and international asset transfer and remittance services entail a significant money laundering risk due to their convenience, reliability and speed. In addition, the use of such services does not require any planning or expertise. In some circumstances, the threshold for suspicious activity can be crossed even if no money actually changes hands. For example, a customer may try to open an account with falsified identification or the transaction may involve other suspicious elements.

3.1 Indicators related to customer profile

- ✓ Activity on an account does not match the customer information or customer profile.
- ✓ Several individuals with no apparent family or business relationship have the right to use an account.
- ✓ An account owner does not engage in any commercial activity, but the account is used for various business-related transactions.
- ✓ An individual has opened several accounts into which many small deposits are made.

- ✓ A customer has several bank accounts or foreign accounts without any commercial, legal or tax- or accounting-related rationale.
- ✓ A customer's reported occupation or income is not in proportion to the level or type of transactions. For example, a student or unemployed individual makes or receives a large number of bank transfers or withdraws large sums of cash on a daily basis.
- ✓ Preliminary information provided by a customer and their goals for the use of products or services do not correspond to their actual behaviour in the field of investments, for example.
- ✓ A customer or their family members or representatives use foreign accounts without a valid reason.
- ✓ An individual is a party to transactions with individuals or entities on international or national sanction or asset-freezing lists.
- ✓ An individual owns foreign assets that have not apparently been declared to the tax authorities.
- ✓ Transfers are made in small sums evidently designed to avoid due diligence or the reporting obligation.
- ✓ A customer or their business operations have connections to countries and territories with geographical risks. For example, the customer engages in business with companies or individuals in conflict zones or operates in a country with a high corruption risk.
- ✓ A customer seems to avoid sanctions in their transactions by operating through neighbouring countries or regions.
- ✓ A customer or their next of kin or business partner is a politically influential person.
- ✓ A customer specifically requests information on the bank's anti-money laundering practices.
- ✓ A customer is in a hurry and wants to perform transactions on an especially/exceptionally tight schedule.

3.2 Transactions on customer accounts

- ✓ One or several deposits are suddenly made into a dormant account, followed by daily cash withdrawals or unusual domestic or international payments to accounts in Finland or abroad.
- ✓ Funds are transferred to an individual without providing any information on the payer or individual on whose behalf the transaction was carried out, even though providing such information would have been expected.
- ✓ A sum equal to a sum recently transferred from the account is returned to the account.
- ✓ Several transfers appear connected due to a common place of performance, recipient or another feature.
- ✓ Several transfers appear connected to one or several countries with a high drug trafficking risk.
- ✓ Several small payments are simultaneously made, which indicates a larger sum being divided into smaller components.
- ✓ There is no clear and appropriate financial or commercial rationale for a financial transaction, or the transaction is economically incompatible with the account holder’s business and occupation.

3.3 Cash funds

- ✓ An account is actively used for cash deposits.
- ✓ Several large cash deposits are made into an account.
- ✓ Several large cash withdrawals are made from an account.
- ✓ Several related automated deposits are made within a short period.
- ✓ Deposits are made through several branches of the same financial institution or simultaneously by different individuals in the same branch office.
- ✓ Bank notes with a suspect appearance are used to make a deposit (e.g. very old or dirty notes).

- ✓ Large cash deposits are made into the account of an individual or entity even though corresponding business transactions would normally be carried out with other means of payment.
- ✓ Cash deposits are made into an account that is not normally used for such business transactions.
- ✓ Sums of cash remaining just below the identification or reporting threshold are systematically withdrawn or deposited.
- ✓ An exceptionally large payment is made into an account and immediately withdrawn in cash.
- ✓ Cash withdrawals are made on the same day at several branch offices and/or cash machines.
- ✓ A representative of a company makes large or unusual cash withdrawals.
- ✓ Large sums of cash are withdrawn from a pension savings account.
- ✓ There are transactions involving large sums of cash on an account.

3.4 International transfers

- ✓ Large cash deposits are made for the purpose of making international transfers.
- ✓ A customer receives several large domestic transfers into their personal account, and these transactions are soon followed by international transfers corresponding to the received sums.
- ✓ Large and significant international transfers are made into a bank account without any commercial rationale.
- ✓ A customer transfers funds from a pension/savings account into a recently opened account and soon thereafter makes international transfers.
- ✓ The parties to a transfer are more interested in how fast the bank can carry out the transfer than the cost of the transaction, without any underlying commercial rationale.
- ✓ International transfers are made from an individual’s account into a number of foreign accounts registered under the same name, often located in tax havens.

- ✓ International transfers to high-risk countries are made.

3.5 Loans

- ✓ A loan is repaid prematurely with sums disproportionate to the customer's income.
- ✓ A customer obtains a loan from an unknown source.
- ✓ Several loan applications appear to be connected.
- ✓ The same or similar methods are used to take out several bank loans.
- ✓ The repayment schedule for a loan is unrealistic.
- ✓ A customer reports the source of funds as a loan from a source that is difficult to verify.
- ✓ A loan is obtained in cash.
- ✓ The purpose of a loan seems suspicious.
- ✓ The required documents between contracting parties have not been prepared or presented.
- ✓ The interest rate agreed between contracting parties differs significantly from the market rate.
- ✓ Interest or instalments are not paid, or the payment schedule is not observed.
- ✓ The origins of assets used as collateral for a loan are unknown and the collateral is paid in cash, for example.
- ✓ Instalments are paid by individuals not connected to the customer relationship.
- ✓ The funding requested by a customer does not correspond to their financial situation.

3.6 Information and documents

- ✓ Documents and information requested for customer due diligence are incomplete.

- ✓ Documents presented for customer due diligence are in poor condition. For example, a passport or other form of identification is worn or damaged; damaged documents may have been tampered with.
- ✓ Transactions by a customer stop within a relatively short period of time after the bank has requested documents to justify the flow of funds.
- ✓ A customer attempts to use falsified documents.
- ✓ Unexplained inconsistencies are discovered during the customer due diligence or identification process regarding matters such as prior or current country of residence, the country that issued the passport, the visited countries recorded on the passport, or documents obtained for verifying the customer's name, address and place of employment.
- ✓ When opening an account, a customer refuses to provide the information requested by the financial institution, attempts to limit the amount of information given or provides information that is misleading or difficult to verify.
- ✓ The same address has been given as the home address of several individuals when opening accounts or carrying out transfers.
- ✓ The same or highly similar documents have been presented by several different customers or for several transactions.
- ✓ A customer frequently changes addresses, establishes new companies or makes other repeated changes whose accuracy and purpose are difficult to verify.
- ✓ A customer, in particular a legal entity, provides the documents required for the due diligence or verification process with exceptional speed and completeness.

3.7 Legal entities

- ✓ Assets of a company are gradually transferred into another account, raising suspicions of a 'transit account'.
- ✓ Numerous incoming and outgoing transfers with no apparent commercial or financial rationale are made on a corporate account.

- ✓ Tax refunds that are large in proportion to the company's known business activities are paid into a corporate account and withdrawn in cash.
- ✓ An account opened by a local company is used for deposits and withdrawals in foreign currencies that are not linked to its business activities.
- ✓ A company's financial statements indicate a marked increase in turnover in a short period of time, often in connection with a spike in the volume and monetary amount of transactions on its bank accounts.
- ✓ There is no connection between a company's business goals and activities generating cash flow.
- ✓ There is a discrepancy between the turnover reported by a company and the performed business transactions.
- ✓ There are material deficiencies or contradictions in the documentation presented to the bank.
- ✓ A legal entity that opened an account is registered at the same address as other legal entities or organisations for which the same individual(s) has/have the authority to sign documents, but there is no evident commercial or legal rationale for the arrangement.
- ✓ Unexpectedly large deposits are made into the account of a recently established legal entity.
- ✓ No information on a company is available from public sources.
- ✓ A company uses an email address provided by a commonly used service provider (Gmail, Hotmail, Yahoo), and the customer acts mysteriously or avoids direct contact.
- ✓ The company has partners or business operations in geographical high-risk areas.

3.8 Corruption

Corruption is the abuse of influence for gain. It refers to misconduct and unethical behaviour in both the public and private sectors. Corruption requires reciprocity and the simultaneous presence of three elements: a position in which influence can be exercised, its abuse and private interests. The European Commission estimates that corruption costs the EU economy around

EUR 120 billion per year. Corruption has serious consequences, slowing down economic development and undermining democracy, human rights and competition.

According to research, corruption in Finland does not manifest as bribery on the street, but rather in large-scale structural forms that are difficult to detect and often occur where businesses interact with the authorities and as part of other forms of white-collar crime. Areas of particular risk include the construction industry, public procurement and tendering, urban planning, political decision-making and party/election funding. Foreign trade and sports are also key areas vulnerable to corruption. Typical manifestations of Finnish corruption are the giving and receiving of unjust benefits, conflicts of interest and favouritism. Corruption also manifests in the form of unethical decision-making outside the formal framework. Corruption can also occur among individuals who cannot be considered to be in a politically influential position.

Corruption and money laundering are often linked, and in many cases the corruption does not come to the attention of the authorities until in connection with other suspected criminal offences. The obligation of obliged entities to perform customer due diligence and to detect and investigate suspicious transactions under the Act on Preventing Money Laundering and Terrorist Financing also acts as a means of exposing corruption. Corruption is sometimes equated with bribery even though the phenomenon also includes fraud, embezzlement and insider trading. For more information and anti-corruption tools, see the korruptiontorjunta.fi website managed by the Ministry of Justice at korruptiontorjunta.fi: Combating corruption through transparency and impartiality.

The prevention of corruption requires extensive cooperation in both the public and private sectors. In Finland, the coordinating authority is the Ministry of Justice.

- ✓ Recently established companies are awarded major public contracts.
- ✓ The same company or companies with the same responsible persons or contact details are consistently awarded the majority of public contracts.
- ✓ A contractor, subcontractor and/or client are linked to each other on the basis of the same address, telephone number or IP address, for example.
- ✓ An individual uses shell companies and companies registered in countries with simplified registration procedures.

- ✓ A private company makes bank transfers to a politically influential individual, their next of kin or a company managed by them.
- ✓ A high-level public official or official with decision-making authority receives funds from the accounts of companies or individuals, and the transfers seem disproportionate to the official's professional activities or position.
- ✓ Payments other than normal salary payments are made to the bank account of an individual employed by a sports club or a sponsoring company or the next of kin of such an individual.
- ✓ An individual holding a public office or a position of trust receives consultancy fees or similar payments from a private company while in office or in the position of trust or within a short period after leaving office or the position of trust.
- ✓ Abnormal cash deposits are detected in the account transactions of an individual holding a public office or a position of trust.

4 Terrorist financing

Careful customer due diligence and monitoring of customers are some of the key factors in identifying and combating terrorist financing. Proper customer due diligence allows the detection of changes in both account usage and other consumption behaviour.

Terrorism or parties supporting terrorism should not be directly linked to any religion, nationality, culture or ethnic group. However, the risk-based assessment of a customer should take into account the whole picture, so if an individual's behaviour suggests radicalisation, extremism or violence that may be related to their religion, nationality or ethnic background, these factors should also be taken into account.

FATF divides the indicators of terrorist financing into seven different categories:

1) Customer behaviour
2) Asset profile
3) Geographical risks
4) Consumption habits
5) Product and service risks
6) Risks associated with non-governmental organisations
7) Risks associated with trade and business

Customer behaviour

- ✓ Indications of extremism, radicalisation or violence can be found in the account transactions of a customer, information from public authorities, social media and public sources about the customer.
- ✓ A customer's login and location information is in or near a high-risk area.
- ✓ In addition to sanction lists, screening of other individuals must take place.
- ✓ A customer is interested in the reporting obligation and other official measures.
- ✓ An agent acts on behalf of a customer without any valid reason.
- ✓ A customer is or has been a foreign combatant, or has links to foreign combatants and related activities.

Asset profile

- ✓ There is an increase in deposits and money flow, often from unknown/unexplained sources.
- ✓ The amount and type of cash flow does not correspond to the normal income level of a customer's occupation.
- ✓ Several individuals give the same contact details.
- ✓ Several individuals have joint/shared accounts without any family connection or another conventional reason.

Geographical risks

No precise definition of high-risk areas with regard to terrorist financing exists, but countries in which terrorists operate or reside can be considered to present a high risk. Countries that may finance terrorist activities can also be considered high-risk areas.

High risks are also presented by countries with deficient anti-money laundering and terrorist financing measures. In addition to the above, even certain European countries have an elevated risk related to terrorist financing due to their location and recent history. More than 800 foreign combatants have left Albania, Bosnia-Herzegovina, Kosovo, Macedonia and Serbia to fight in the Syrian civil war. The Balkan states have also been one of the main routes from Europe to conflict zones and back for a long time.

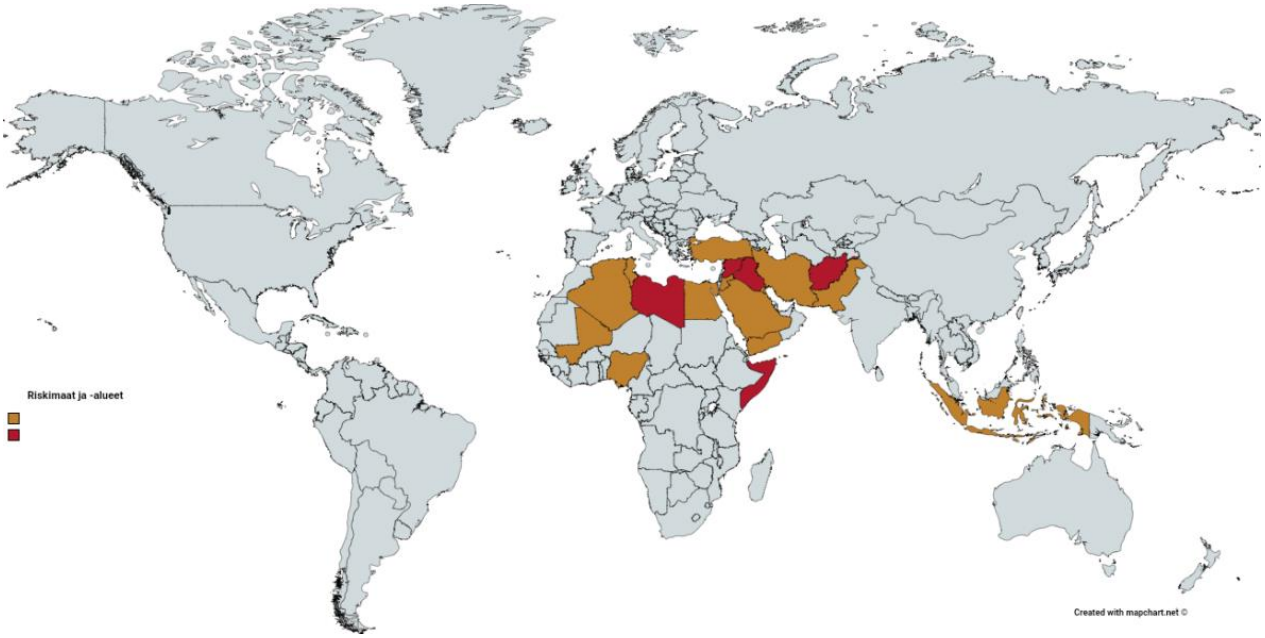
Highest-risk countries/regions with conflicts, areas controlled by terrorist organisations, and the neighbouring countries of such countries:

- Syria and Iraq, neighbouring countries Turkey, Iran, Jordan, Syria, Saudi Arabia, Kuwait, Yemen

- Libya, neighbouring countries Tunisia, Algeria, Egypt

- Afghanistan, neighbouring country Pakistan

- Somalia, Nigeria, Mali, Indonesia, the Philippines



Consumption habits

- ✓ There are payments related to travel.
- ✓ A customer purchases visas, flights and coach tickets to and from transit countries.
- ✓ A customer makes inquiries and contractual amendments related to life assurance.
- ✓ A customer contributes and donates to companies or organisations supporting extremism and violence.
- ✓ A customer makes purchases related to weapons and survival and trekking supplies (tents, weapons, satellite phones, explosives, military surplus goods, etc.).

Product and service risks

- ✓ A customer uses several remittance services.
- ✓ A customer uses several foreign neobanks.
- ✓ A customer uses virtual currencies for fund transfers.
- ✓ A customer uses service providers and payment arrangements outside the traditional payment transaction infrastructure.

Risks associated with non-governmental organisations

- ✓ There is a sudden increase in donations to an NGO for no justifiable reason.
- ✓ An NGO receives large donations from abroad or from entities without a direct connection to the organisation.
- ✓ There is atypical use of financial instruments.
- ✓ There are transactions, expenses or activities that do not fall within the scope or are incompatible with the operations of an NGO.
- ✓ There is an unexplained mismatch in expenses, transactions, donations, beneficiaries or other activities (only a few individuals as beneficiaries, transactions not correlating with the beneficiaries/donations, assets of the NGO in individuals' accounts, etc.).
- ✓ There is international networking of NGOs, e.g. operations under the same name in several countries.

Risks associated with trade and business

- ✓ A company does business with an individual with possible links to terrorist financing.
- ✓ A customer establishes several companies in rapid succession, and the companies remain in operation only for a short period.
- ✓ A company makes purchases not related to its sector (e.g. camping and military surplus purchases).
- ✓ A company has a large number of individuals with account access rights and authority to sign for the company.
- ✓ There are fund transfers to high-risk countries.
- ✓ There are fund transfers abroad without any commercial rationale.

5 Payment service providers

The provision of payment services includes a range of services and products related to the execution of payments and the transfer and exchange of funds. According to the national risk assessment, the risk level for payment service providers is 3, i.e. significant. New payment service providers and new technologies in the sector with features that may be challenging to

understand and monitor are considered a risk. Payments are being monitored retroactively and move across borders quickly, even at international level, making it difficult to stop them. Payment services make it easy to switch between currencies, which increases the risk of money laundering.

The Finnish and Swedish Financial Intelligence Units, together with other relevant authorities, implemented an EU-funded Black Wallet project to identify terrorist financing and money laundering risks in the FinTech sector. The project developed and produced a risk indicator list and a number of other publications and guidebooks for both the private and public sector. The project publications are available on the website of the Police of Finland.[11]

- ✓ A customer buys and/or uses several electronic money products.
- ✓ A product designed for one user seems to be used by several individuals.
- ✓ There are regular changes in a customer's identification information.
- ✓ A customer appears to be acting on behalf of someone else.
- ✓ A customer uses a service in an unusual way.
- ✓ A customer's knowledge of a payment recipient seems to be limited.
- ✓ The value of payments made by a customer seems to be inconsistent with the financial situation declared by the customer.
- ✓ Registration for a service is done using an anonymous or disposable email service.
- ✓ A customer's contact details can be linked to more than one profile.
- ✓ A customer has an atypical IP address.
- ✓ A customer often has transactions close to the reporting threshold.
- ✓ Funds are quickly transferred to or from virtual currency platforms.

[11] Reviews and reports on comba<ting money laundering and terrorist financing – Police of Finland

6 Currency exchange

It is known that foreign exchange offices are used for money laundering, but the volume of cases is difficult to estimate. Currency exchange is a common way of laundering money due to its ease and speed. There are plenty of exchange offices, and the services are easily accessible.

- ✓ A customer exchanges a considerable number of large notes for small notes in foreign currencies.
- ✓ A customer exchanges a considerable number of small notes for large ones.
- ✓ A customer gives an implausible explanation regarding the source of their funds.
- ✓ A customer exchanges money for several different currencies.
- ✓ A customer repeatedly exchanges currency without using a bank account.
- ✓ A customer exchanges currency at several different offices within a short period.
- ✓ A customer uses couriers who often work on behalf of different unidentified clients.
- ✓ The amounts exchanged are disproportionate to the income normally generated by the occupation a customer claims to practise.
- ✓ The currency exchange is unusual compared to the normally activities on an individual’s account.
- ✓ There is no commercial rationale for a business transaction or the rationale is incompatible with the type of transaction carried out.
- ✓ A customer repeatedly exchanges amounts just below the reporting threshold.

7 Virtual currencies

Virtual currencies are digital value bearers that are not issued by a central bank. Virtual currencies do not have the same legal status as traditional currencies or cash, although they can be used in the same way as traditional money. According to the national risk assessment, the risk level of the virtual currency sector is very significant.[12]

The Act on Virtual Currency Providers (Laki virtuaalivaluutan tarjoajista 572/2019) entered into force in 2019, which means that virtual currency providers are now included in the scope of the Act on Preventing Money Laundering and Terrorist Financing, and are therefore subject to the reporting obligation. The Financial Supervisory Authority monitors virtual currency providers, and they are required to register with the Financial Supervisory Authority. Provision of virtual currency refers to the issuance of virtual currency and the provision of exchange services, a marketplace or wallet services.[13]

- ✓ A customer makes exceptionally large deposits or withdrawals with no apparent commercial rationale.
- ✓ A customer cannot be identified, refuses to provide the documentation required for identification or provides incomplete information.
- ✓ A customer carries out exceptionally large transactions in relation to their financial status/customer profile, or there is no reliable account of the customer's assets.
- ✓ No information on the origin of funds that have been deposited into a customer's account can be obtained, and the customer resells large volumes of currency.
- ✓ A customer changes their telephone number or address several times within a short period, or unexplained changes occur in their login location data.
- ✓ Several similar small transfers are made within a short period, remaining deliberately below the investigation or reporting threshold.
- ✓ Virtual currencies are exchanged for other virtual currencies and then quickly transferred or withdrawn.

[12] National risk assessment of money laundering and terrorist financing 2021 (valtioneuvosto.fi)

[13] Virtual currency providers – FinTech – Financial sector innovations - www.finanssivalvonta.fi

- ✓ A customer has a high turnover volume between virtual and traditional currencies within a short period.
- ✓ A customer demands to know transaction thresholds or regulatory requirements before opening an account or completing a transaction.
- ✓ An analysis indicates that funds are being transferred into a virtual currency exchange platform from a suspect source such as a mixer service, a black marketplace, an address or service subject to sanctions, an exchange service with a high-risk country of registration, or an exchange service that is otherwise assessed to be of a high risk.
- ✓ A customer's transaction information or addresses are suspicious based on public sources.

8 International trade indicators

FATF and the World Customs Organization (WCO) consider trade-related money laundering to be one of the main ways of transferring and laundering large amounts of illicit funds. International trade is a lucrative choice for money launderers, as it involves a variety of opportunities for money laundering. Methods of trade-related money laundering include over- or under-invoicing, double invoicing, fictitious business transactions and false declaration of goods or their value.

- ✓ Import and transport costs are high in relation to the value of a product.
- ✓ There are major discrepancies between a product's declared value and market value.
- ✓ There are major discrepancies between delivered goods and their descriptions.
- ✓ There are major discrepancies between the amount indicated on an invoice and the related insured value.
- ✓ An invoice sum does not match the payment.
- ✓ The origin of goods and the destination of funds (or vice versa) are different.

- ✓ The country involved is not known to import or export the products in question.
- ✓ A recently established company imports or exports large volumes of goods.
- ✓ The value, quantity or type of goods is incompatible with the profile of a supplier or buyer.
- ✓ Supplier or buyer companies include companies registered in tax havens.
- ✓ A company engages in double invoicing, with several invoices drawn up for the same products.
- ✓ The transport method is incompatible with the nature or size of a product.

9 Casinos and gambling

According to the national risk assessment, the overall risk level for gambling activities in both mainland Finland and the Åland Islands is at level 2, i.e. moderately significant. The use of foreign gambling companies, as well as the related fragmentation of control measures and challenges in obtaining information are considered as the main risks of money laundering. An increasing proportion of gambling revenue is generated from online gambling, where the identification of the customer and traceability of the transactions reduces, but does not entirely eliminate, the risk of money laundering. For example, customers can recycle illicit funds via gambling accounts by first depositing the funds into the account and then quickly withdrawing them, thus making the funds look like gambling proceeds.

- ✓ A customer gambles, loses or transfers disproportionate amounts compared to their annual income or general financial situation.
- ✓ A customer's gambling behaviour changes drastically.
- ✓ The purpose of a customer's gambling or money transfers does not appear to be winning.
- ✓ A customer's gambling behaviour is unusual in the customer bracket.

- ✓ A customer deposits funds into a gaming account, but the funds are not drawn from and deposited into the same account.
- ✓ A customer has a bad credit record but high gambling volume.
- ✓ A customer appears to purposefully gamble, transfer funds or purchase chips just below the reporting threshold.
- ✓ The gambling of two or more customers appears coordinated.
- ✓ A customer uses for gambling an account that is not in their name (e.g. a corporate account or the account of a minor).
- ✓ A customer frequently changes the account into which gambling proceeds are deposited.
- ✓ A customer transfers large amounts into their gambling account but gambles only a little if at all.
- ✓ A customer receives or buys chips or tickets or accepts money from a third party.
- ✓ A customer gives or sells chips or tickets to a third party.
- ✓ A customer buys or redeems chips or tickets for disproportionate sums.
- ✓ A customer buys chips or gambles on slot machines with unusually large amounts of small notes.

10 Insurance products

Insurance products and life assurance policies that enable the customer to invest funds into the financial system and potentially conceal their origin involve a risk of money laundering. The risk increases if the insurer accepts premium payments in cash or if the policy can be assigned or prematurely terminated, returning the accumulated funds to a different account or a different individual.

- ✓ A customer cancels a policy and requests the funds to be transferred to a third party.
- ✓ A customer terminates a policy despite significant tax consequences or other cancellation fees.

- ✓ A customer immediately withdraws or transfers the funds released from a cancelled insurance product.
- ✓ A customer signs a contract for a significant sum and the related payments are made from abroad.
- ✓ A customer is particularly interested in the early surrender of a product and the amount that would be made available to them.
- ✓ A customer pays their insurance premiums in one cash instalment, and the paid amount is clearly disproportionate to the customer's income.
- ✓ A customer purchases an insurance product without paying attention to its investment targets or performance.
- ✓ A customer replaces the original beneficiary with an individual with no apparent connection to the customer.
- ✓ A customer cannot be identified or refuses to provide the information required for identification.
- ✓ A customer insures significantly valuable assets disproportionate to the customer's financial status.

11 Lawyers and legal services

The multinational risk assessment carried out by the European Commission ascribes a significant money laundering risk to lawyers and other providers of legal services. Lawyers must have adequate policies, procedures and monitoring regimes in place to decrease the risk of money laundering and terrorist financing. In addition to the contents of the commission, the risk factors can be related to the client and their business partners. The geographical risks discussed above must also be taken into consideration. Offenders can use the services of lawyers for the management of client accounts, for real estate transactions or to establish companies, for example. The involvement of a lawyer can give an act the appearance of legality. If a transaction involves representatives from several sectors (e.g. a real estate transaction), every party has an independent obligation to report suspicious transactions.

- ✓ A client cannot be identified, refuses to provide the documentation required for identification or provides incomplete information, or uses documents that appear falsified, especially identification documents.
- ✓ A client demands suspicious business transactions to be carried out quickly.
- ✓ A client has changed legal advisers several times in a short period without a valid reason.
- ✓ A client's previous legal advisers have refused the assignment or a previous adviser has terminated their contract with the client.
- ✓ An adviser based far from the client or from the location of the transaction is chosen with no commercial rationale.
- ✓ A client is prepared to pay an abnormally large fee.
- ✓ A client commissions a lawyer for a civil case which is settled almost immediately and the settlement is paid through the law firm's client account.
- ✓ Damages or contractual penalties are paid for no apparent reason.
- ✓ There is considerable under- or over-invoicing by a company or a client.
- ✓ A client wants to pay a transaction price or other payment related to a contract or business transaction in cash.
- ✓ A client wants to be invoiced through a foreign company with no apparent connection to the client.
- ✓ The legal arrangements related to a client's business are disproportionately complex with regard to the nature of the business.
- ✓ A property is bought or sold for considerably more or less than its fair value.
- ✓ A client deposits cash into a client account in several instalments, adding up to a significant sum.
- ✓ A client uses the details of or purports to represent a company in which the client has no actual role.

- ✓ An individual acting as a managing director lacks the required competence or business experience.
- ✓ A foreign national with no link to Finland invests in real estate in Finland, or the investments are disproportionate to the client's socio-economic status.
- ✓ Payments are made into a client account in a client's name from an individual, financial institution or company residing or registered in a country known for enhanced banking secrecy, a favourable taxation system or the production of narcotics, or a country which is included on the FATF list of non-cooperative countries or territories.[14]
- ✓ A client has established or wants to establish several companies within a short period, either in their own name or on behalf of another individual, without any apparent taxation-related, legal or commercial rationale.
- ✓ A client participates in unusual activities that do not appear connected to the client's occupation or the ordinary course of their business, and the client is unable to offer a satisfactory explanation for these activities.
- ✓ A client wants to establish or acquire a company with a suspicious business purpose or no apparent relation to the client's normal professional or business activities and is unable to offer a satisfactory explanation for this.

12 Real estate agents

The national risk assessments places real estate agents at risk level 2, i.e. the risk is moderately significant. The overall risk level for letting agencies is 1, i.e. less significant. The risk is compounded by the fact that a typical real estate transaction involves representatives from various sectors, who typically trust in the control and monitoring of each other. One of the most significant risks is over-reliance on the credit institution to perform customer due diligence, monitor the customer, trace the origin of the funds and identify the customer or the customer's beneficial owners. Parties active in the sector may assume that the credit institution has already verified the origin

[14] See Section 2.6.

of the customer's funds to a sufficient extent, in which case they will not question or investigate the matter themselves.

Every obliged entity in a business relationship has an independent obligation to report suspicious transactions. Obliged entities accumulate different types of information on their clients and thus have different capacities to identify potentially suspicious transactions. The variety of entities involved in a real estate transaction make it possible to conceal the origins of illicit funds, while simultaneously enabling the transfer of large sums in a single payment. Obliged entities should keep in mind that both parties of the transaction, i.e. the real estate agent's client and the buyer, must be examined for signs of suspicious activity.

- ✓ A client buys a property without actually seeing it.
- ✓ A transaction is completed in a hurry.
- ✓ A client wants to pay the purchase price entirely or largely in cash.
- ✓ A client buys a property in the name of a third party with no apparent connection to the client.
- ✓ A first-home buyer is buying an exceptionally valuable property without any financing.
- ✓ A property is sold for significantly more than its market value.
- ✓ A property is sold for significantly less than its market value.
- ✓ A property is repeatedly sold with unusual profit margins and there is no clear rationale for these transactions.
- ✓ A client refuses to provide the agent with the number of the account into which the transaction price was or will be paid.
- ✓ A client uses different names on the contract of sale, transaction and payment.
- ✓ A client employs advisers for the transaction, and their fees are disproportionate compared to the value of the transaction.
- ✓ A client or their next of kin has a criminal record, bad credit history or a prohibition to pursue a business.

13 Accountants, auditors and tax advisers

The money-laundering risks of accountants, auditors and tax advisers are partly common with those of the legal profession, and the services of these professionals have also been employed in money laundering activities. The multinational risk assessment considers accountants to be subject to a significant money laundering risk. The falsification of accounts, double invoicing and tax havens have also been identified as key risks in the national risk assessment. In their own risk assessments, accounting and audit service providers have highlighted the limits of their detection capacities. Even though accountants have access to receipts related to cash flow entries, the authenticity of these documents is difficult for them to assess. According to the risk assessments, fake receipts prepared for illicit fund transfers have most likely been modified to appear legal before being delivered to the accounting firm, making their authenticity difficult to verify.

If representatives of different sectors participate in a business transaction, each entity has an independent obligation to report suspicious business transactions. This is particularly relevant in the case of accountants, auditors and tax advisers, as they often provide several services, and a single company can be subject to different reporting obligations based on the provision of different products and services.

- ✓ A client is constantly changing accountants.
- ✓ The sales or business volumes of a recently established company are unusually high.
- ✓ A client appears to live beyond their means or the client's income is disproportionate to their professional activities.
- ✓ A company has a complex legal structure, which is an often-used method for concealing the beneficial owners.
- ✓ A company uses fake purchase and sales agreements to move funds without any actual goods or services changing hands, or uses other fake remedies such as contractual penalties.
- ✓ A company has no employees and this is unusual in light of its purported activities.
- ✓ A company deposits and withdraws large sums of cash.

- ✓ The costs of business transactions and contracts have not been itemised and the related receipts are incomplete.
- ✓ A company pays various consultancy fees, particularly to companies registered in tax havens.
- ✓ A company's receipts appear fake, and similar types of receipts have raised suspicions before.
- ✓ A company makes payments to companies or deposits funds into accounts in tax havens.
- ✓ A company receives deposits made with combinations of payment instruments that are atypical for normal business operations.
- ✓ A company makes bank deposits that are not posted as turnover.
- ✓ Suspected offenders or their partners are involved in business operations or transactions.
- ✓ Payments do not translate into revenue or sales.
- ✓ A company pays dividends with no financial rationale.
- ✓ The number of a company's partners is disproportionate to the nature of the business.
- ✓ An audit of a company's accounts raises suspicions or reveals embezzlement.
- ✓ There are particularly complex loan arrangements and irregularities between a creditor and a debtor.

14 Tax havens and non-cooperative countries

Cases of money laundering often involve companies and financial institutions operating in tax havens. Therefore, obliged entities should pay particular attention to business transactions and customer relationships with such connections. According to the OECD's definition, tax havens have low tax rates and high levels of banking secrecy, but no international treaties on the exchange of taxation information or legislation on transparent ownership.

Panama, the Bahamas, Bermuda and the Cayman Islands have traditionally been considered as tax havens.[15]

The European Commission has published a blacklist of territories that refuse to cooperate with the EU in taxation matters and are not committed to the OECD's measures for the prevention of tax evasion. The countries on the list include Bahrain, Barbados, Macau, the Marshall Islands, Mongolia, Namibia, Panama, Saint Lucia, Samoa, South Korea, Trinidad and Tobago, Tunisia and the United Arab Emirates. There is also a grey list of countries that have made commitments to change their tax policies and are being monitored by the EU. Such countries include Switzerland and Thailand.[16]

Other geographical risk areas include regions with extensive corruption or other criminal activity, and countries on which the EU or UN has imposed sanctions. Obliged entities should pay particular attention to customers and business transactions with connections to such countries. The countries on the lists maintained by the FATF and European Commission have deficiencies in their anti-money laundering and terrorist financing legislation or measures. Obliged entities are required to apply enhanced customer due diligence to customers and business transactions with connections to such countries. According to the national risk assessment, front companies, false receipt trading and related arrangements are particularly easy and affordable to implement via tax havens.

- ✓ Business operations involve companies based in tax havens, and the sole purpose of the arrangement appears to be concealing the actual operators of the business. For example, the individuals in charge of the company are not familiar with the basics of the line of business.
- ✓ Companies with links to tax havens are used in business operations, and the arrangements are notably complex with regard to the nature and scope of the business activities.
- ✓ A company was established in a tax haven without an apparent commercial rationale or other valid reason.
- ✓ Transit accounts are often used for funds of foreign origin, which are then quickly transferred to the accounts of companies based in tax havens.

[15] Veroparatiisit - vero.fi
[16] st15429en17.pdf (europa.eu)

- ✓ Proceeds from the sale of a company have been invested in a tax haven.

15 Straw man indicators

Dummy purchasers or ‘straw men’ can be used as concealed intermediaries in a variety of legal acts. A straw man can serve as a dummy buyer in a real estate transaction, as a dummy insurer in the insurance sector or as a dummy executive of a company on behalf of an individual prohibited from operating a business. Having a straw man conclude legal acts on behalf of another individual conceals the real beneficiary of the act. There are multiple reasons for using straw men such as circumventing legislation, avoiding official intervention or concealing the actual ownership arrangements and beneficiaries for political or other reasons. As straw men are often used for dishonest purposes, they can also give cause to suspect the origin of the funds used for the transaction. If an entity suspects that a straw man is being used, refusing to conclude the legal act could be wise. Straw men can be difficult to detect, however, especially if the transaction takes place online.

- ✓ A legal act or business transaction is incompatible with a customer’s profile or appears unconnected to the customer’s business or situation, and the obliged entity suspects that the customer is acting on someone else’s behalf.
- ✓ An individual acting on behalf or in the name of a company is not familiar with the company’s operations, or their competence is not at a level required by the business transactions being carried out.
- ✓ A customer’s business transactions make it seem like a third party is using the customer’s account.
- ✓ International transfers are made through a straw man posing as the account holder or an individual with a power of attorney to use the account.
- ✓ A customer uses a straw man for a real estate transaction without a valid commercial or legal rationale.

16 Non-governmental organisations

Risks related to NGOs are a special area in the fight against money laundering and terrorist financing. NGOs often operate in countries in crisis or conflict, or in their neighbouring territories, which increases the terrorist financing risks related to their activities. The indicators can be roughly divided into donations, expenses, transactions and the managers and employees of NGOs.

- ✓ Large donations are made to an NGO by a foreign company or other entity without any direct connection to the organisation.
- ✓ There is a surprising growth in the number of small donations to an NGO without any logical explanation.
- ✓ Donations, particularly ones made in cash, add up to large sums.
- ✓ There are several cash deposits into a private account (or indications of a need to transfer cash to an individual in a high-risk territory), with their purpose recorded as “humanitarian purposes”.
- ✓ The majority of an NGO’s donations or funds originate from abroad or are transferred abroad into a country that is inconsistent with the donor’s financial information.
- ✓ Donations for charity are made into a private individual’s account and then transferred to organisations with links to terrorism.
- ✓ An NGO that does not engage in any humanitarian work sends money to a high-risk country.
- ✓ An NGO uses funds in an irregular manner for expenses that are not related to the organisation’s activities.
- ✓ Transactions point to a construction project, but the recipient of the funds has no connections to the NGO or the construction industry.
- ✓ A third party that is not a member of the NGO involved has paid for products instead of an importer.
- ✓ The official expenses of an NGO are disproportionate to its activities.
- ✓ An NGO has transactions that do not correlate with the information provided by the recipients of the aid.

- ✓ Large transactions are made within a short period, involving several organisations and unexplained connections (e.g. same names, contact details or accounts).
- ✓ The majority of collected funds is transferred into high-risk countries.
- ✓ Requests for transactions with terrorist-listed entities or connected entities are identified in an NGO's operations.
- ✓ There are recurring private donations to the account of an NGO, which are then transferred to an individual or legal entity.
- ✓ There are only credit or cash transactions on the account of an NGO.
- ✓ Several individuals who have no business relations with the NGO have the authority to sign for an NGO, or the individuals with such authority are changed frequently.
- ✓ There are large deposits or payments to the private accounts of the founders of an NGO and frequent cash withdrawals from the founders' accounts.
- ✓ Information on the source of funds transferred into the accounts of an NGO or its employees is incomplete.
- ✓ The management or employees of an NGO give false information on the use of funds before travelling to a conflict zone, e.g. where cash withdrawals were made before or during the trip.

17 Hawala

Hawalas are a sub-category of remittance services, often operating in a limited geographical area or within a specific ethnic group in North and East Africa, the Middle East, and South and South-East Asia. In Finland, the largest and best-known hawala network is based on the Somali community. Hawalas are used in countries such as Somalia, where social instability and protracted conflicts have created a demand for such a remittance service. According to a review by the World Bank, approximately 1.2–1.4 billion US dollars are sent to Somalia annually via hawalas, and these cash flows are a lifeline for millions of Somalis, especially those living in remote areas.

In a hawala, money is usually collected from customers through bank transfers or in cash, with the corresponding amount being paid to the recipient by

a local hawala in the destination country. The hawala agent charges a commission for each remittance, and a part of the commission is paid to the "parent company".

In Finland, such activities are usually arranged through a company, association or personal account, and the business is franchising-based. The majority of remittances originate from Finland and are made to individuals in Islamic states. As the activity is often directed to abroad, the agent operating the hawala in Finland will incur a "debt" to either the parent company or agents operating in other countries. The books are balanced by making fairly large deposits to the parent company's bank account, usually based in the Arab Emirates, China, Djibouti, Hong Kong, Kenya, Singapore, Turkey or Qatar, most often as an international payment. Hawalas also annually transfer tens of millions of euros in cash from Finland to settle accounts abroad, nowadays typically to Turkey, but also to some extent to the United Arab Emirates and Djibouti.

Hawala activities are mostly based on the Islamic culture and mutual trust in the remittance system. Serving as a hawala agent requires a licence from the Financial Supervisory Authority. In addition to the hawala agents registered for supervision by the Financial Supervisory Authority, it is estimated that there are several legal entities operating hawala in Finland without the required licence. According to the national risk assessment, the risk level for hawalas is 4, i.e. very significant. The highest risk is posed by hawala agents not registered with the Financial Supervisory Authority.

In Finland, hawala is a legal but licensed form of business, and registered licensed hawala agents are subject to the reporting obligation. The main risks associated with hawalas are money transfers to crisis and conflict zones, lack of clarity on the intended use of the funds, large amounts of cash, the unlicensed activities and shortcomings in terms of the reporting obligation. In recent years, hawalas have started using accounts outside the EEA for their operations, which further increases the risk. Private individuals can also engage in hawala activities without establishing a company. Weaknesses have been identified in the customer due diligence processes of hawala agents: customers may be identified based on their name and telephone number alone.

- ✓ Private individuals transfer plenty of funds to a hawala business account or to a current account of an individual linked to a hawala.
- ✓ A large sum of money is collected into the account of an individual and then transferred to a business account or abroad.

- ✓ Account transfers refer to a specific geographical area abroad or a foreign name.
- ✓ Account transfers refer to a “loan”, “payment” or “debt” without an identifiable debt or loan relationship.
- ✓ Account transfers refer to “money”, “loan”, “payment”, “exchange” or “shipment” in Somali, Arabic, Persian, Dari, Pashto, Turkish, etc.
- ✓ Account transfers directly and unambiguously refer to the sending of money to a specific individual or to a specific geographical area.
- ✓ Large amounts of cash, possibly originating from a cash collection, are regularly deposited without any credible explanation.
- ✓ Cash is used in another ambiguous and suspicious manner, such as for large cash purchases.
- ✓ Large amounts of cash are withdrawn without a credible explanation, whereby cash may be transported abroad to maintain the balance sheet of a hawala system.
- ✓ There are large foreign payments to countries such as Turkey, the United Arab Emirates, Qatar, etc.
- ✓ There are large payments to international hawala “parent companies”.
- ✓ There are transfers into accounts outside the EEA the owner of which is identified as the hawala itself.
- ✓ An individual has a high volume of cash and bank transfers even though their main source of income is social security or low wage income, which suggests that they may be a hawala fundraiser.
- ✓ According to open sources, a legal entity has links to an international hawala organising remittance.
- ✓ A licensed legal entity acts as a local agent for an international money transfer company in Finland, in which case it is possible to acquire the license to act as an agent and still carry out money transfers through the hawala system.

Sources:

EU list of non-cooperative jurisdictions for tax purposes, European Council, EU list of non-cooperative jurisdictions for tax purposes - Consilium (europa.eu)

Hallituksen esitys eduskunnalle laiksi rahanpesun ja terrorismin rahoittamisen estämisestä, laiksi rahanpesun selvittelykeskuksesta sekä eräiksi niihin liittyviksi laeiksi 228/2016 vp (Government proposal on the Act on Preventing Money Laundering and Terrorist Financing, the Act on the Financial Intelligence Unit and certain associated acts)

High-Risk Jurisdictions, FATF, Documents - Financial Action Task Force (FATF) (fatf-gafi.org)

High risk third countries, European Commission, High risk third countries and the International context content of anti-money laundering and countering the financing of terrorism (europa.eu)

Jurisdictions under Increased Monitoring, FATF, Documents - Financial Action Task Force (FATF) (fatf-gafi.org)

International sanctions, Ministry for Foreign Affairs, Pakotteet - Ulkoministeriö (um.fi)

Kansallinen rahanpesun ja terrorismin rahoittamisen riskiarvio (National risk assessment of money laundering and terrorist financing), Finnish Government 2021 (valtioneuvosto.fi)

Sanctions by country, Ministry for Foreign Affairs, Pakotteet maittain - Ulkoministeriö (um.fi)

Selvitys terrorismin rahoittamisen ominaispiirteistä (Review on the characteristics of terrorist financing), Financial Intelligence Unit 2021

Veroparatiisit (Tax havens), Finnish Tax Administration, https://www.vero.fi/tietoa-verohallinnosta/verohallinnon_esittely/toiminta/vastuullisuus/verovaj/veroparatiisi/

Virtuaalivaluutan tarjoajat (Virtual currency providers), Financial Supervisory Authority, Virtuaalivaluutan tarjoajat – FinTech –

Finanssialan innovaatiot (Innovations in the financial sector) – www.finanssivalvonta.fi