POLIISI

Letter
06/02/2026
Document: ID-2641073
Subject: POL-2025-152385

Written guidance for entities subject to reporting obligations regarding the prevention of money laundering and terrorist financing in the gambling sector

Contents

Definitions 3
1 Introduction 3
1.1 Purpose and objective of the guidelines 3
1.2 General information on the prevention of money laundering and terrorist financing in the gambling sector 4
2 Regulation 5
2.1 FATF Recommendations 5
2.2 EU Anti-Money Laundering Regulation and Anti-Money Laundering Directives 6
2.3 AMLA Regulation 6
2.4 National legislation 6
3 Money laundering and terrorist financing 7
3.1 What is money laundering? 7
3.2 What is terrorist financing? 8
4 National and supranational risk assessment and supervisor-specific risk assessment 8
4.1 National risk assessment 9
4.2 Supranational risk assessment 10
4.3 Supervisor-specific risk assessment 10
5 Risk assessment by the reporting entity and risk-based approach 11
5.1 Risk assessment by the reporting entity and risk management methods 11
5.2 Identification and assessment of risk factors 14
5.3 Risk factors that must be identified and assessed 15
5.3.1 Risk classification of customers 15
5.3.2 Products and services 16
5.3.3 Transactions 17
5.3.4 Delivery channels 18
5.3.5 Countries and geographical regions 18
6 Understanding the customer 19
6.1 General information on knowing your customer and risk-based assessment 19
6.2 Procedures for knowing your customer 20
6.2.1 Standard customer due diligence measures 20

6.2.2 Enhanced customer due diligence 20
6.3 When should customer due diligence measures be carried out? 21
6.3.1 Establishment of a customer relationship 21
6.3.2 Ongoing monitoring of the customer relationship and changes in material circumstances 22
6.3.3 Measures taken regularly during the customer relationship to get to know the customer 23
6.3.4 Transactions exceeding a certain threshold 24
6.3.5 Suspicion of money laundering or terrorist financing 24
6.3.6 Suspicious nature of previously received customer information 24
6.3.7 Large, unusual and/or irrational deposits 25
6.4 Know your customer requirements relating to compliance with sanctions regulations and freezing orders 25
6.5 Source of funds 27
6.6 Insufficient customer information 28
7 Reporting to the Financial Intelligence Unit 29
7.1 General information about the Financial Intelligence Unit 29
7.2 Reporting a suspicious transaction 29
7.3 Indicators of suspicious transactions in gambling operations 30
8 Use of intermediaries 31
9 Training 32
10 Internal control and whistleblowing system 34
10.1 Internal control 34
10.2 Whistleblowing system 35
11 More on the prevention of money laundering and terrorist financing 35

Definitions

FATF (Financial Action Task Force) – An intergovernmental body that develops international standards to combat money laundering, terrorist financing and the proliferation of weapons of mass destruction

AMLA Anti-Money Laundering Authority – The EU's anti-money laundering authority PEP

Politically Exposed Person – A politically influential person

VAS Source of Funds Declaration

STR Suspicious Transaction Report FIU / RAP Financial Intelligence Unit /

Financial Intelligence Unit SNRA Supra-National Risk Assessment NRA

National Risk Assessment

1 Introduction

1.1 Purpose and objective of the guidelines

These guidelines are intended for gambling operators holding a licence in Finland, their employees and other relevant stakeholders. The content of the guidelines is relevant to all gambling operators applying for or holding a licence, and is also useful for their agents.

The guidance is not a detailed manual on how an individual gambling operator should operate, but it provides an overview and a summary of the obligations of gambling operators in accordance with the key elements of anti-money laundering regulations. It also outlines possible approaches to risk-based working and provides examples of effective measures to prevent money laundering and terrorist financing.

Users of these guidelines must always assess whether the guidelines are applicable in a specific case. Gambling operators must also always take into account, among other things, the provisions of the Money Laundering Act, as well as the regulations and general guidelines issued by the supervisory authority regarding the prevention of money laundering and terrorist financing. Gambling operators must also take into account the regulator-specific risk assessment, as well as the National Risk Assessment (NRA) and the Supranational Risk Assessment (SNRA), in their operations.

The supervisory authority publishes up-to-date information on the prevention of money laundering and terrorist financing through its own channels, such as its own risk assessment, guidelines or updates thereto. The supervisory authority also provides information on changes to the national

and supranational risk assessments. Gambling operators must actively monitor the supervisory authority's communications. In addition, the supervisory authority recommends that gambling operators actively monitor the rahanpesu.fi website. The website publishes up-to-date information on the prevention of money laundering and terrorist financing in Finland.

1.2 General information on the prevention of money laundering and terrorist financing in the gambling sector

The Finnish gambling market is undergoing major changes, as gambling operations will be partially brought under a licensing system under the new Gambling Act (10/2026). Applications for exclusive rights and gambling licences (hereinafter 'licences') under the Gambling Act may be submitted from 1 March 2026, and operations may commence from 1 July 2027. The Gambling Administration of the National Police Board will act as the supervisory authority until 30 June 2027. From 1 July 2027, the Licensing and Supervisory Authority will act as the supervisory authority.

Gaming operators are subject to reporting obligations under the Money Laundering Act (Act on the Prevention of Money Laundering and Terrorist Financing 444/2017). The Money Laundering Act shall also apply, where applicable, to a business operator or entity that transmits participation notifications or payments, if the gambling operator has delegated the task of customer identification and reporting to another business operator or entity.

In this context, it should be noted that, at the time of writing these guidelines, a comprehensive reform of the national Money Laundering Act is underway. This comprehensive reform implements the EU's 6th Anti-Money Laundering Directive. The new Money Laundering Act will come into force, for the most part, on 10 July 2027, at which point the EU Anti-Money Laundering Regulation will also begin to apply. The new Money Laundering Act and the Anti-Money Laundering Regulation will bring about changes to the obligations of those subject to reporting requirements. **These guidelines have been drafted in the light of current anti-money laundering legislation, and the supervisory authority will issue new guidance when the new Act and the Anti-Money Laundering Regulation come into force.**

The aim of the Money Laundering Act is to prevent money laundering and the financing of terrorism, to facilitate the detection and investigation of such activities, and to improve the tracing and recovery of the proceeds of crime. The key principle of anti-money laundering regulation is to prevent business activities from being exploited for money laundering and terrorist financing. At the same time, it must be ensured that the conduct of effective business is not unnecessarily restricted. Balancing these interests requires the licence holder to adopt **a risk-based approach**.

The risk-based approach must permeate all of the gambling operator's work related to the prevention of money laundering and terrorist financing; in other words, the measures must be proportionate to the risks associated with the gambling operator's activities. The risk-based regulation under the Money Laundering Act enables gambling operators to focus their measures effectively on those areas where the risk of money laundering and terrorist financing is greatest.

A risk-based approach requires gambling operators to have a thorough understanding of the risks associated with money laundering and terrorist financing, particularly within the gambling sector, and to be able to

make informed decisions. This, in turn, requires the development of expertise through, for example, training, guidance, professional advice and practical experience.

The Money Laundering Act obliges gambling companies to take active measures to prevent money laundering and terrorist financing. This obligation includes, among other things, the active monitoring of customers, the identification of suspicious transactions and the reporting of such transactions to the authorities. Failure to comply with and/or violation of the obligations under the Money Laundering Act may lead to consequences such as administrative sanctions, revocation of the operating licence or criminal proceedings.

In the national risk assessment of money laundering and terrorist financing published by the Ministry of Finance in 2021, the money laundering risk in the gambling sector is assessed as level 2 **(moderately significant)**, which is mainly due to large stakes, large winnings, high turnover and the use of cash. Money launderers often accept potential losses, meaning that a person may lose significant sums whilst any potential winnings may appear to be legitimate income. For these reasons, gambling can be an attractive money laundering method for criminals. See Chapter 4 for more on the national risk assessment.

Due to the moderately significant risk, it is important that gambling operators have adequate anti-money laundering and counter-terrorist financing practices in place, commensurate with the nature and scale of their operations.

The importance of complying with the obligations under the Money Laundering Act is emphasised by the fact that the supervisory authority may impose an administrative fine, a penalty payment or a public warning on a gambling operator as an administrative sanction for neglecting or breaching the obligations under the Money Laundering Act. Under the new Gambling Act and the 6th Anti-Money Laundering Directive, the supervisory authority may also revoke a gambling operator’s licence.

2 Regulation

2.1 FATF Recommendations

The Financial Action Task Force (FATF) is a global organisation comprising over 200 countries and jurisdictions. They have committed to having their measures to combat money laundering, terrorist financing and the proliferation of weapons of mass destruction assessed by evaluators supported by the FATF Secretariat in Paris. Finland has been a member since 1991.

The FATF has adopted 40 recommendations for the prevention and combating of money laundering and terrorist financing. As a member state, Finland is obliged to comply with the FATF’s recommendations.

The provisions of the Money Laundering Act are largely based on the EU Money Laundering Regulation and EU directives (Money Laundering Directives), which in turn are based on the FATF recommendations.

2.2 The EU Anti-Money Laundering Regulation and the Anti-Money Laundering Directives

Finland, along with other EU countries, is facing changes to anti-money laundering rules. The Member States adopted a new legislative package on 31 May 2024. Its aim is to create a more detailed and harmonised regulatory framework. Among other things, the legislative package means that a large part of the Fourth Anti-Money Laundering Directive will be replaced by the so-called Anti-Money Laundering Regulation, which is directly binding and directly applicable law in Member States. The Anti-Money Laundering Regulation will apply from 10 July 2027.

Those parts of the Fourth Anti-Money Laundering Directive that were not transferred to the Regulation have been replaced by the Sixth Anti-Money Laundering Directive. The provisions of the Sixth Anti-Money Laundering Directive will be implemented in national anti-money laundering legislation and will apply from 10 July 2027.

2.3 AMLA Regulation

In addition to the EU Anti-Money Laundering Package, a new authority, the Anti-Money Laundering Authority (AMLA), has been established at EU level through the so-called AMLA Regulation. AMLA was officially established in July 2024 and commenced operations in 2025 in Frankfurt, Germany. Most of the agency’s tasks will commence in 2025–2026, with the exception of the direct supervision of reporting entities in the financial sector and certain tasks relating to sectors other than the financial sector, which will begin in 2028.

As financial crime is cross-border in nature, the new authority will enhancethe effectiveness of the anti-money laundering and counter-terrorist financing regime by establishing a mechanism, in coordination with national supervisory authorities, to ensure that reporting entities comply with anti-money laundering and counter-terrorist financing obligations in the financial sector. The AMLA is also tasked with supporting sectors outside the financial sector and coordinating the financial intelligence units of member states.

In addition to its supervisory powers, and to ensure compliance with requirements, the AMLA imposes financial penalties on selected reporting entities in cases where directly applicable requirements are breached and the breaches are serious, systematic or repeated.

2.4 National law

These guidelines are based on the national Act on the Prevention of Money Laundering and Terrorist Financing (2017/444).

At the time of writing, a comprehensive reform of the national anti-money laundering legislation is underway to implement the 6th EU Anti-Money Laundering Directive. This comprehensive reform will bring significant changes to national legislation.

In addition to national law, the EU Anti-Money Laundering Regulation is directly applicable law in Finland. The application of the Anti-Money Laundering Regulation will largely commence in July 2027.

The supervisory authority will issue new guidance on the new Anti-Money Laundering Act and the EU Anti-Money Laundering Regulation closer to the date of their entry into force.

3 Money laundering and terrorist financing

3.1 What is money laundering?

The purpose of the Money Laundering Act is to prevent and deter the misuse of the financial sector, the gambling sector and many other sectors for money laundering or terrorist financing.

The definition of money laundering is set out in Section 4 of Chapter 1 of the Money Laundering Act, according to which money laundering refers to the activities referred to in Sections 6–10 of Chapter 32 of the Criminal Code (39/1889).

In money laundering:

- the funds are of illegal origin.
- the aim is to circulate the money through the legal payment system.
- the aim is to conceal the true nature, origin or owners of the funds.

Money laundering refers to activities in which funds obtained through criminal means are circulated through the legal payment system with the aim of concealing or obscuring the true nature, origin or ownership of the funds. Money laundering therefore requires a predicate offence. A predicate offence may be any act punishable by law from which the perpetrator has derived financial gain.

Money laundering also includes the receipt, use, conversion, disposal, transfer, brokering or possession of criminal proceeds. The person must have the intention to launder money, i.e. the intention to obtain a benefit, assist the offender or conceal the illegal origin of the property. Money laundering also involves concealing and obscuring the true nature, origin, location or control or rights over property obtained through crime.

Money laundering is considered to consist of three stages: placement, layering and integration. Initially, the funds are brought into the legitimate financial system, for example as cash deposits. After this, attempts are made to conceal the illegal origin, for example through complex transactions. The money is, for example, moved through multiple accounts and across multiple countries to distance it further from its origin. Finally, the funds are brought back into the legitimate economy.

Preventing money laundering can also help prevent other forms of crime, as money launderers may use the proceeds to finance further criminal activities. Money laundering is often part of organised and international crime. Money laundering can threaten the stability, reliability and competitiveness of the financial system. Instability can, for example, increase the costs of loans, payments and insurance, and the effects may be felt more widely across the economy.

The methods of money laundering vary and can be simple or more complex. It is not just a matter of cash transactions. Money that already exists within the financial system can also be vulnerable to money laundering.

3.2 What is terrorist financing?

According to Section 4 of Chapter 1 of the Money Laundering Act, the financing of terrorism refers to the activities referred to in Sections 5, 5a and 5b of Chapter 34a of the Criminal Code. The financing of terrorism involves the acquisition or collection of funds for terrorist activities. It is not merely a matter of providing funds. The financing of terrorism also encompasses the collection, transfer and receipt of money used for terrorism. Terrorism is often financed through legitimate means, which makes it particularly difficult to detect.

In the financing of terrorism:

- funds may be of legal or illegal origin.
- money is acquired or collected for terrorist activities.
- It is also a criminal offence to finance a terrorist group or an individual terrorist, or to attempt to do so.

The stages of terrorist financing include the collection, transfer and use of funds. Terrorism is mainly financed with funds obtained from legitimate sources, and financial transactions take place via bank transfers, in cash or through money transfer services. Financial transactions take place between several different countries.

To combat terrorism and prevent the financing of terrorism, funds may be frozen in respect of a natural or legal person in accordance with the provisions of the Act on the Freezing of Funds for the Purpose of Combating Terrorism (325/2013). The purpose of freezing assets is to prevent the subject of the decision from channelling funds for terrorist purposes. In Finland, the National Bureau of Investigation makes decisions on the freezing of funds and maintains a public register of such decisions. The decision to freeze funds is enforced by the enforcement authority.

To combat terrorism and prevent the financing of terrorism, sanctions are also imposed, which in practice mean restrictions on economic or other cooperation with designated entities. Sanctions are intended to influence activities deemed to pose a threat to, for example, security. In the fight against terrorism, sanctions may take the form of financial sanctions, such as the freezing of assets. The Ministry for Foreign Affairs lists, among other things, anti-terrorism sanctions on its website.

4 National and supranational risk assessments and risk assessments by supervisory authority

Both national and supranational risk assessments relating to the prevention of money laundering and terrorist financing have been published, and these are updated regularly. The supervisory authority has also published a supervisor-specific risk assessment. Gambling operators must familiarise themselves with the risk assessments and other published guidelines and guides, and incorporate them where applicable

its own risk assessment, which it must draw up on the basis of its own business model. Further information on the gambling operator's risk assessment can be found in Chapter 5 of these guidelines.

4.1 National risk assessment

As part of measures to prevent money laundering and terrorist financing, Finland must prepare a national risk assessment. The risk assessment must identify and evaluate the risks of money laundering and terrorist financing in Finland. The risk assessment must take into account the European Union's supranational risk assessment prepared by the European Commission. According to Section 1 of Chapter 2 of the Money Laundering Act, responsibility for preparing the national risk assessment lies with the Ministry of Finance and the Ministry of the Interior. In addition, numerous different bodies are involved in preparing the risk assessment, comprising national competent authorities, supervisors under the Money Laundering Act, authorities subject to the duty of care, and private sector operators.

The 2021 National Risk Assessment on Money Laundering and Terrorist Financing has been prepared under the coordination of the Ministry of Finance and the Ministry of the Interior. The risk assessment describes the threats, vulnerabilities and risks of money laundering and terrorist financing across all sectors subject to reporting obligations, as well as in the activities of non-profit organisations (the NPO sector). In addition, the risk assessment examines the risks of money laundering and terrorist financing in relation to selected phenomena.

In connection with the risk assessment, a national action plan for the 2021–2023 risk assessment of money laundering and terrorist financing has been drawn up. The action plan sets out the measures aimed at mitigating the risks identified in the risk assessment. The risk assessment and the action plan form a whole that reflects Finland's national understanding of the risks of money laundering and terrorist financing and the means of managing them.

The 2023 partial update of the National Risk Assessment on Money Laundering and Terrorist Financing has been prepared under the coordination of the Ministry of Finance and the Ministry of the Interior. The partial update of the risk assessment describes the threats, vulnerabilities and risks of money laundering and terrorist financing in the sectors subject to the highest risk reporting obligations. In addition, the partial update examines the risks of money laundering and terrorist financing in relation to selected phenomena. The partial update does not replace the 2021 risk assessment, but merely supplements it.

In connection with the partial update of the risk assessment, the national action plan for the risk assessment of money laundering and terrorist financing for 2024–2025 has been updated. The action plan sets out the measures aimed at mitigating the risks identified in the risk assessment. The risk assessment and the action plan form a whole that describes Finland's national understanding of the risks of money laundering and terrorist financing and the means of managing them.

The national risk assessment will undergo a comprehensive update during 2025–2026. The new national risk assessment is scheduled for publication in early 2026. The supervisory authority will inform gambling operators of the content and changes to the national risk assessment.

4.2 Supranational risk assessment

Article 6 of the Fourth Anti-Money Laundering Directive required the European Commission to carry out an assessment of the risks of money laundering and terrorist financing affecting the European Union's internal market that are associated with cross-border activities. This risk assessment is referred to as the Supra-National Risk Assessment (SNRA).

The Directive requires the Commission to update the report every two years, or more frequently if necessary. The Commission published the latest SNRA report and its annexes on 27 October 2022.

The risk assessment identifies, analyses and evaluates the risks of money laundering and terrorist financing that affect the European single market and relate to cross-border activities at Union level. The risk assessment covers key risks to the Single Market across a range of sectors, as well as horizontal vulnerabilities that may affect these sectors.

On this basis, the document sets out guidelines on risk-mitigating measures to be followed at both EU and national level. It also contains recommendations for various obliged entities and authorities.

4.3 Supervisor-specific risk assessment

Under Section 2 of Chapter 2 of the Money Laundering Act, the competent supervisory authority must prepare a risk assessment of the risks of money laundering and terrorist financing associated with the reporting entities falling within its supervisory remit.

The supervisor-specific risk assessment serves several purposes and objectives, all of which aim to help prevent money laundering and terrorist financing in the gambling sector. The aim is to map and identify risks, assess their likelihood and impact, and present methods for managing the risks of money laundering and terrorist financing in gambling operations. The objective of the risk assessment is to identify money laundering risks associated with gambling and to assess them.

It is impossible to identify all risks, but the aim is to identify the most likely and significant money laundering risks associated with gambling. Furthermore, the aim of the risk assessment is to propose some measures to mitigate these risks. For this reason, the risk assessment analyses the risks and also presents risk management measures. The risk assessment evaluates the likelihood, impact and severity of the identified risks.

The risk assessment is a tool for supervisory activities. It enables the supervision of anti-money laundering and counter-terrorist financing to be targeted, among other things, at those activities where the risks have been identified as being the most significant. In supervisory work, this targeting of supervision is referred to as risk-based supervision. On the other hand, the identification and assessment of smaller risks are also significant in gaining an overall picture and understanding the comprehensive risks of money laundering and terrorist financing associated with gambling.

A risk assessment is the supervisory authority's view of the factors and events threatening gambling operations in relation to money laundering and terrorist financing. The risk assessment also serves as a tool for gambling operators. Gambling operators can, among other things, compare the regulator-specific risk assessment with the risk assessment they have carried out on their own operations and assess whether their gambling operations have taken into account all the risks presented in the supervisory authority's risk assessment, as well as how the risks and control measures have been assessed by the regulator.

Gambling operators can view the regulator-specific risk assessment and its appendices on the police website.

The supervisory authority will draw up a new risk assessment for the prevention of money laundering and terrorist financing in connection with the transition to the licensing system.

Gambling operators should note that the risk assessment specific to the supervisory authority is a separate document from these written guidelines.

5 Risk assessment and risk-based approach for entities subject to reporting obligations

5.1 Risk assessment and risk management methods for reporting entities

The Money Laundering Act requires gambling operators to implement risk-based measures to prevent the misuse of their business for money laundering and terrorist financing.
This means that gambling operators' resources are primarily allocated to areas where the risks of money laundering and terrorist financing are greatest in their business operations. A gambling operator must therefore understand its business model in order to identify and assess the associated risk of being misused for money laundering and terrorist financing. The risk may change if the gambling operator alters its business model, and this may lead to either an increase or a decrease in risk.

To carry out risk-based work, a gambling operator must therefore conduct a risk assessment of its own business. Risk assessment is a key part of all other work to prevent money laundering and terrorist financing. It must form the basis for business practices and other measures to prevent money laundering and terrorist financing. The scope of the risk assessment depends on the size and nature of the business.

The risk assessment must be documented. It must describe how the gambling operator's products and services could be used for money laundering or terrorist financing, and how high the risk is that this will occur. **All factors that may influence the risks of money laundering and terrorist financing must be taken into account in the risk assessment**. In particular, the gambling operator must consider the type of products and services offered, customers, transactions, distribution channels and geographical risk factors.

A gambling operator's risk assessment must address both the risk of money laundering and the risk of terrorist financing. For example, a particular gambling game offered by a gambling operator may pose a high inherent risk of money laundering but only a low risk of terrorist financing.

A gambling operator must update its risk assessment regularly. To ensure that the risk assessment always reflects the gambling operator's current risk profile and is as relevant and up-to-date as possible, the risk assessment must generally be reviewed at least once a year or whenever significant changes occur in the gambling operator's business model or in legislation. The gambling operator must also review its risk assessment if changes occur in national and supranational risk assessments or in the regulator-specific risk assessment that may affect the gambling operator's inherent risk.

This requires the gambling operator to have an understanding of the actual threats and vulnerabilities. Consequently, the business must possess expertise in money laundering and terrorist financing within the Finnish context. This is a fundamental factor in the effective application of a risk-based approach and requires gambling operators to continuously monitor the latest reports on money laundering and terrorist financing.

When preparing a risk assessment, a gambling operator must take into account the nature, size and scope of its operations. Taking the above factors into account, a gambling operator must have adequate policies, procedures and controls in place to mitigate and effectively manage the risks of money laundering and terrorist financing. The policies, procedures and controls must include at least:

1) the development of internal policies, procedures and controls;
2) internal audit, where this is justified given the nature and scale of the reporting entity's operations.

The gambling operator must draw up the aforementioned operating principles, procedures and controls, and monitor and develop the related measures. If the gambling operator subject to the reporting obligation is a legal person, the board of directors, a general partner or another person in a similar position within senior management must approve the operating principles, procedures and controls referred to in Chapter 2, Section 3(2) of the Money Laundering Act, and monitor and develop related measures.

A gambling operator's risk assessment for the prevention of money laundering and terrorist financing must be a separate and independent document. The gambling operator must therefore note that it is not sufficient to include anti-money laundering measures in its general risk assessment or, for example, in the self-monitoring plan referred to in Section 35 of the new Gambling Act. The risk assessment and any amendments thereto must be submitted to the supervisory authority upon request without undue delay.

In addition to a risk assessment, gambling operators must have risk-based risk management methods in place to combat money laundering and terrorist financing. The purpose of risk management methods is to prevent risks identified in operations. It is therefore important that a gambling operator's general anti-money laundering risk assessment and risk management methods are closely linked.

Risk management procedures must cover at least the following areas:

- customer due diligence measures
- monitoring and reporting
- processing of personal data
- staff suitability assessment and staff training
- compliance with regulations and internal control.

In addition to risks, gambling operators must also take into account threats and vulnerabilities in their operations and include them in their risk assessments.

Risk refers to the probability of money laundering or terrorist financing occurring, as well as the severity of the associated harm or consequences.

Risk = Threat × Vulnerability Example:

If a gambling product allows large sums of money to be transferred quickly without effective supervision (vulnerability), and criminals seek to exploit this (threat), the risk is high.

A threat refers to an actor, event or mechanism that may seek to exploit a gambling operator as a vehicle for money laundering or terrorist financing.

A threat may be, for example:

- a criminal individual or network
- a money laundering method (e.g. chip dumping in poker)
- a phenomenon affecting the operating environment (e.g. organised crime).

A threat does not mean that a crime has already been committed, but rather that there is an intention or possibility of it occurring.

Vulnerability refers to a characteristic of a gambling operator or its products and processes that enables or facilitates money laundering or the financing of terrorism.

Vulnerabilities may include, for example:

- inadequate customer due diligence
- ineffective or inadequate monitoring
- slow response to suspicious transactions
- products that allow money to be transferred easily without any genuine gaming purpose.

5.2 Identification and assessment of risk factors

When assessing the risks of its business model, a gambling operator must identify and assess its inherent risk of being misused for money laundering and terrorist financing. The risk assessment of a gambling operator's business model thus consists of two parts – the identification of risk factors and their assessment.

A gambling operator must identify all material risk factors associated with its business model. In order for a gambling operator to identify the material risk factors that may affect its risk of being misused for money laundering and terrorist financing, it must first conduct a thorough analysis of its business model and understand the vulnerabilities of its gambling servicesfrom the perspective of money laundering and terrorist financing.

The scope and nature of risk factors depend on the nature and size of the gambling operator, and on how it has chosen to organise its business model.

When a gambling operator identifies risk factors associated with its business model, it must take into account national and supranational risk assessments as well as other relevant sources. It can be challenging to identify which specific features of a business model may pose a risk in relation to money laundering and terrorist financing. In this context, the purpose of the national and supranational risk assessment is to help the gambling operator obtain information on sector-specific risk factors. Similarly, other relevant sources, such as these guidelines and the supervisor-specific risk assessment, can help gambling operators identify the material risk factors associated with their business.

Once a gambling operator has identified its inherent risk factors, it must, in accordance with a comprehensive approach, assess the extent to which the identified risk factors may expose it to money laundering and terrorist financing. A gambling operator may choose how it expresses its assessment of its inherent risk factors. Risk factors may be assigned weightings and classified**,** for example**, as low, medium and high**. The weighting of risk factors may be based on an assessment of probability and consequences. This means that, when assessing the risk of money laundering and terrorist financing, a gambling operator may emphasise the likelihood of a particular risk factor materialising, as well as its potential consequences.

The gambling operator must carry out the assessment in such a way that it can subsequently use the risk assessment as an operational tool to understand to what extent and in which areas it may be exposed to money laundering and terrorist financing. In this way, the gambling operator can target its mitigating measures at the areas of greatest risk.

As mentioned earlier, the gambling operator must assess the risk associated with each inherent risk factor in its business model separately. A mere assessment of the general risk level, which may relate to several risk factors, is not sufficient. By assessing the risk separately for each individual risk factor, the gambling operator gains a better understanding of whether its individual risk factors pose a low or significant risk of being exploited for money laundering and terrorist financing.

5.3 Risk factors that must be identified and assessed

A gambling operator's risk assessment must cover, at a minimum, the risk factors relating to its customers, products and services, transactions, distribution channels and geographical areas.

This means that a gambling operator's risk assessment must not be limited solely to the areas mentioned, but must reflect and cover all parts of the business model. For example, a gambling operator must also identify and assess the inherent risks associated with the company's organisation. In this context, the gambling operator may assess the risk that its own employees are involved in money laundering or terrorist financing. Furthermore, risk factors may be associated, for example, with the use of agents.

The scope of the risk assessment depends on the gambling operator's specific business model. If a gambling operator has a broad business model, for example offering a wide variety of gambling products both online and at physical outlets, this places greater demands on the content and scope of the risk assessment. In such cases, the gambling operator's business model includes several risk factors that must be taken into account in the prevention of money laundering and terrorist financing. On the other hand, if a gambling operator has a more limited and restricted business model, the risks it faces are lower.

Regardless of the size and scope of its operations, a gambling operator must carry out a fundamental analysis of how its specific business model may be exposed to money laundering and terrorist financing in the Finnish context.

5.3.1 Customer risk classification

Customer risk classification must be carried out on the basis of a general risk assessment of the business and the information obtained by the gambling operator about the customer. When a new person registers as a customer with a gambling operator, a risk level must be assigned to them.

In risk-based work, **measures must be proportionate to the risks**. For example, verifying annual income or occupation may be sufficient for normal-risk customers, whereas in high-risk cases, additional verification and direct contact with the customer are required to ascertain the source of funds.

Risk factors relating to a gambling operator's customers refer to the types of customers with whom the gambling company deals or to whom it is otherwise exposed. For example, a gambling operator may have customers who appear on the European Commission's list of high-risk third countries, or who are politically exposed persons (PEPs) or family members of politically exposed persons.

The gambling operator's specific business model determines which types of customers it must assess. In Finland, under Section 21 of the Gambling Act, a gambling operator may offer electronic gambling and register as a customer only a natural person who has a permanent address in mainland Finland. However, the gambling operator must be aware that even though it only accepts customers from Finland, foreign customers may still attempt to

circumvent a gambling company's restrictive measures, for example by using false documents or VPNs.

With the entry into force of the new Gambling Act, the provision of gambling services at physical locations, for example through agents, does not require the customer to have a permanent address in mainland Finland. Gambling operators must also take into account the potential risks arising from such customer relationships in their risk assessments and customer risk classifications. Gambling operators must also note that mandatory customer identification applies to gambling at physical outlets as well. Anonymous gambling is not permitted.

Under Finnish gambling legislation, a gambling operator is permitted to accept only natural persons as customers. Consequently, the gambling operator's risk assessment regarding customer types does not cover companies or beneficiaries.

Once a gambling operator has identified all relevant customer types, it must assess the risk associated with each customer group regarding their potential misuse of the business for money laundering and terrorist financing. A gambling operator may include general information and experience regarding these customers in its assessment. By examining its customers, the gambling operator can-gain an overview of the types of customers it has and whether the general behaviour of customers affects the extent to which a particular customer group creates an inherent risk of the gambling company being misused for money laundering and terrorist financing.

The gambling operator must continuously monitor the customer's risk classification and, where necessary, adjust the risk level. If a customer's risk is assessed as higher than at the time of establishing the business relationship, the gambling operator must obtain further information about the customer and, where necessary, intensify ongoing monitoring and supervision. If a customer is assessed as posing a lower risk, monitoring and supervision need not be as comprehensive or take place as frequently.

In order to carry out a customer risk assessment, a gambling operator must always undertake, as a minimum, measures relating to customer due diligence and checks for politically exposed persons (PEPs) and sanctions. The gambling operator must obtain information on the purpose and nature of the business relationship, regardless of the customer's risk category. This information must also be assessed on an ongoing basis. For example, a gambling operator may obtain information on the customer's annual income or the personal nature of the bank account linked to the customer relationship. In addition, the origin of the funds used for gambling must be ascertained. The origin of funds refers to more detailed information on the customer's financial situation and the source of the sums deposited into the gaming account and the funds used for gambling. Further details on customer due diligence measures can be found in Chapter 6 of these guidelines.

In the case of high-risk customers, the gambling operator must carry out enhanced customer due diligence measures in addition to those mentioned above. For more information on enhanced customer due diligence, see Chapter 6 of these guidelines.

5.3.2 Products and services

The gambling operator must identify and assess the risk factors associated with the products and services it offers. From the perspective of money laundering and terrorist financing, not all gambling activities are equally susceptible to abuse. Certain types of games clearly

a higher risk than others. A gambling operator must identify these high-risk forms of gambling and take them into account in its risk assessment, customer monitoring and reporting practices, and possibly impose stricter identification and gambling restrictions on them.

Gambling is particularly susceptible to money laundering when it involves, for example, the following elements:

- the opportunity to make large one-off investments
- the fast pace of the game, high performance speed
- the opportunity to play against other people
- the opportunity to make moves that are deliberately designed to benefit another player
- the use of multiple accounts or third parties
- insufficient monitoring of player behaviour or money transfers
- use of cash
- if the gambling product is not entirely based on chance but includes elements such as skill.

Betting, poker and casino games have become established as the highest-risk forms of gambling**.**

Once a gambling operator has assessed the individual risk factors associated with a specific gambling product, it must also assess the risk of the product itself on the basis of this risk assessment.

The gambling operator must identify and assess the risk factors for all its gambling products. If a gambling company offers several different variants of the same gambling product, these variants must be assessed separately if they differ significantly from the operator's other products.
If the products offered by the gambling operator differ only for cosmetic reasons, there is no need to carry out a separate risk assessment.

5.3.3 Transactions

The gambling operator must identify and assess the risks associated with the payment solutions it uses. The gambling operator must therefore understand which payment solutions customers may use when playing the games it offers.

For example, the gambling operator must take into account that a payment method may be a suitable means of concealing the origin of funds. The gambling operator must also consider the extent to which, or the ease with which, a payment solution can be misused by another person. The gambling operator must also examine whether the payment solution permits fast and large transactions.

Once the gambling operator has assessed the individual risk factors associated with a specific payment solution, the operator must also assess the risk of the payment solution itself based on the assessment of these individual risk factors.

The gambling operator must generally assess the risks for all payment solutions used by the operator. If a gambling operator uses several different types of e-wallets or bank cards, all of which share the same general characteristics and are otherwise similar, the gambling operator does not need to assess the risks separately for each variant of the payment solution. In such cases, it is sufficient for the gambling operator to assess the general risk of the entire payment solution type.

Gambling operators offering multiple deposit and withdrawal options must be particularly vigilant regarding the possibility of funds being transferred to different accounts. One way to mitigate the risks of money laundering and terrorist financing is to **ensure that customers can only withdraw funds to the bank account from which the deposit was originally made**. In this way, the gambling operator can ensure that the customer's financial activities remain consistent, as well as manage and mitigate risks. However, the gambling operator must note that the aforementioned approach alone does not guarantee that deposits made into the gaming account are legally obtained. Gaming operators cannot rely solely on net deposits or previous gaming winnings without separately verifying the origin of the funds. **Simply returning previous gaming winnings to a gaming account does not automatically mean that the funds are lawful**.

5.3.4 Delivery channels

A gambling operator must identify and assess the risks associated with the distribution channels it uses. A gambling operator must therefore carry out a risk assessment of how it chooses to make its gaming products available to its customers and how the gambling company otherwise interacts with customers.

This may, for example, mean that the gambling operator makes its gaming products available online or that it sells its gaming products physically at a land-based casino or gaming hall. It may also mean that the gambling operator sells its gaming products physically through external and internal retailers, or that the operator's products are linked to or accessed via a gaming account or self-service terminals.

Regardless of the gambling operator's business model, it must assess the extent to which its delivery channels may contribute to the misuse of its business for money laundering and terrorist financing.

5.3.5 Countries and geographical areas

A gambling operator must identify and assess the risks associated with countries and geographical areas. Geographical risks must, among other things, be taken into account in the gambling operator's customer risk classifications, as a customer's connection to a specific geographical location may affect their inherent risk. The gambling operator must therefore assess the risks that different countries may pose from the perspective of money laundering and terrorist financing.

Gambling operators must take into account the risks associated with countries and geographical regions when selecting destinations for their gaming offerings. In this assessment, gambling operators should, for example, consider whether a country has strategic shortcomings in preventing money laundering and terrorist financing. In this context, it is relevant to examine whether the country is on the European Commission's

list of high-risk third countries or on the FATF's grey and blacklists. Gambling operators must not select destinations for gaming from countries on the FATF's blacklist or grey list.

6 Know Your Customer

6.1 General information on know your customer and risk-based assessment

Adequate customer due diligence is essential for preventing and combating money laundering and terrorist financing. Customer due diligence is currently regulated primarily in Chapter 3 of the Money Laundering Act.

The fundamental requirement of the Money Laundering Act is that gambling operators must know their customers. This applies to all gambling operators. The purpose of customer due diligence procedures is to ensure that the gambling operator knows who its customers are and the purpose of the customer relationship.

If a gambling operator is unable to carry out the measures for knowing the customer set out in Chapter 3 of the Money Laundering Act, it may not establish a customer relationship, conduct a transaction or maintain a business relationship. The customer due diligence measures set out in Chapter 3 of the Money Laundering Act must be complied with throughout the customer relationship, based on a risk-based assessment.

Knowing the customer is important so that the gambling operator understands the customer's usual behaviour and can thus identify unusual behaviour and changes in the customer relationship. The gambling operator must respond if it detects changes in the customer relationship, for example if the customer's gambling behaviour or volume changes. The gambling operator must establish procedures to enable it to detect and respond to signs of money laundering or terrorist financing.

The gambling operator must carry out customer due diligence procedures at least in the following situations:

- when a customer registers
- when the customer's material circumstances change
- on a regular basis during the customer relationship
- when a customer's stake and/or withdrawal of winnings amounts to at least €2,000 in a single transaction or in linked transactions
- if there is any suspicion of money laundering or terrorist financing
- if there are concerns regarding previously obtained customer information.

The scope of the measures depends on the complexity of the service or product and the associated risks. The more complex the product or business relationship, the more comprehensive the measures required to know the customer and prevent money laundering.

6.2 Procedures for knowing the customer

6.2.1 Standard customer due diligence measures

To fulfil the obligation to know the customer, reporting entities must carry out all of the following measures:

- identifying the customer and verifying their identity
- assessing and understanding the purpose and intended nature of the business relationship or individual transactions and, where necessary, obtaining information relating to them
- verifying whether the customer is subject to targeted economic sanctions
- assessing the nature of the client's business and occupation, and, where necessary, obtaining relevant information
- continuous monitoring of the business relationship, including reviewing transactions throughout the duration of the relationship to ensure that the transactions carried out are consistent with the information held by the reporting entity regarding the customer, their business and risk profile, and, where necessary, the source of funds
- determining whether the customer is a politically exposed person (PEP) or a family member of such a person, or a person known to be a close associate of such a person.

6.2.2 Enhanced customer due diligence

Section 10 of Chapter 3 of the Money Laundering Act provides for enhanced customer due diligence. In certain situations, standard customer due diligence measures are not sufficient; enhanced due diligence measures are required. Enhanced customer due diligence requires the gambling operator to take more thorough measures than usual to verify the customer's identity, business activities and the origin of funds. Enhanced customer due diligence measures must be carried out when the customer, transaction or service involves a higher than normal risk of money laundering or terrorist financing.

Enhanced customer due diligence measures must be implemented, for example, in the following situations:

- The customer is a politically exposed person (PEP) or a close associate of such a person.
- The customer's activities are linked to a high-risk country.
- The customer is carrying out unusually complex or unusual transactions.
- The customer is not physically present during the identification process (e.g. remote banking without in-person identification).

Enhanced customer due diligence may include, for example, the following measures:

- A more in-depth investigation of the customer's background.
- A more detailed investigation of the identity or the structure and beneficial owners of a legal entity.
- Checking for political affiliations.

Assessment of the source of funds:

- The customer may be asked to provide more detailed evidence of the source of the funds (e.g. payslips, documents relating to the sale of assets).

Clarification of the purpose and nature of the transaction:

- What is the purpose of the customer's gambling (e.g. recreational or professional).

Ongoing monitoring of activities:

- Continuous monitoring of the customer's gaming activity and use of services to detect any anomalies.

Management approval for establishing or continuing a customer relationship:

- For example, in the case of a PEP customer, management may need to make a decision on whether to approve the customer relationship.

6.3 When should customer due diligence measures be carried out?

6.3.1 Establishment of a customer relationship

A gambling operator must identify a new customer and verify their identity using a reliable and independent source. In addition to the identification and customer due diligence requirements of the Money Laundering Act, Section 20 of the Gambling Act also requires that a player verify their identity upon registration.

When establishing a customer relationship and throughout the duration of that relationship, a gambling operator may identify and verify the customer's identity by using strong electronic authentication. **The supervisory authority recommends that gambling operators always use strong electronic identification for online gaming**, rather than logging in using, for example, a username and password.

When a customer registers, the gambling operator must collect information on the purpose and nature of the business relationship. The gambling operator must ascertain whether the purpose of the customer's business relationship is recreational gambling or professional gambling. The gambling operator must also ascertain how the customer intends to use the gaming products or services. By determining the expected gaming behaviour, the gambling operator can better assess the frequency of the customer's transactions and the size of their deposits.

The gambling operator must pay attention to the deposit limits set by the customer for online gambling. If a customer indicates at the outset that they play frequently and for large sums, the gambling operator may need to investigate further whether the purpose of the gambling is genuinely for entertainment. This requires additional checks and verification of customer details.

The gambling operator should ask questions when new customers register in order to get to know their customers better from the outset. The questions should focus on the origin and amount of future deposits and on clarifying the intended purpose of the gambling. Such information helps the gambling operator to better understand the purpose and nature of the business relationship and facilitates supervision, monitoring and customer risk classification.

Examples of questions that may be asked when a new customer registers:

- Where does the money you intend to use for gambling come from?
- What was your last annual income?
- What is your occupation?
- Where does your income come from?
- How much do you estimate you will gamble per month?
- What types of games do you estimate you will mainly play?

The purpose of this information is to provide the gambling operator with the basis for assessing the risk associated with the customer and how the customer is likely to behave within the context of their account. This assessment is essential so that the gambling operator can detect deviations from expected behaviour.

In addition to the above, the gambling operator must ascertain whether the customer is a politically exposed person (PEP) or a family member of a politically exposed person. A customer's PEP status always requires enhanced due diligence measures. The gambling operator must also ensure that the customer is not on a sanctions list or subject to asset freezing orders.

6.3.2 Ongoing monitoring of the customer relationship and changes in material circumstances

Section 4 of Chapter 3 of the Money Laundering Act requires gambling operators to carry out monitoring appropriate to the nature and scale of the customer's activities, the stability and duration of the customer relationship, and the risks involved, to ensure that the customer's activities correspond to the gambling operator's experience and knowledge of the customer and their activities. The gambling operator must therefore monitor **the customer relationship continuously throughout the duration of the relationship**. Customer data must be kept up to date and the gambling operator must assess whether the transactions correspond to the customer's risk profile.

The gambling operator must carry out customer due diligence procedures again if the material circumstances of the customer relationship change. An example of a change in material circumstances is if the customer becomes a politically exposed person (PEP) or if the customer's behaviour or gaming habits change significantly. An example of a

a change in a customer's gambling behaviour is if the customer starts to gamble differently or plays different games and for larger sums than before.

Based on the risk assessment, the gambling operator must assess whether the changed circumstances require the collection of new customer information, such as identity details or similar.
The information to be obtained depends on the situation. For example, it may be necessary to re-verify the customer's identity if the gambling operator becomes aware that the customer has changed their name or personal identification number. In some cases, such as a change in the customer's behaviour, simply verifying identity details is not sufficient; the gambling operator must also carry out a source of funds check and take other measures necessary to ensure customer due diligence.

Customer due diligence measures must be carried out as soon as the gambling operator becomes aware of changed circumstances, for example through ongoing monitoring.

Additional measures to improve customer due diligence must also be implemented when a gambling operator detects unusual or suspicious money transfers or activities. The implementation of enhanced due diligence measures does not require the customer to have been classified as high risk.

The ongoing monitoring of customers under the Money Laundering Act is, in part, a similar obligation to the duty of care of a gambling company under Section 34 of the Gambling Act. To fulfil this duty of care, a gambling operator must continuously monitor the customer's gambling behaviour and intervene in the event of unusual or changed behaviour. A gambling operator may, where applicable, take into account the partial similarity of these obligations in its operations and processes.

6.3.3 Measures to identify the customer carried out regularly during the customer relationship

The gambling operator is also obliged to carry out customer due diligence measures regularly during the customer relationship. The purpose of this is to ensure that the customer data held by the gambling operator is up to date and sufficient. In addition to carrying out customer due diligence measures when the customer's material circumstances change, the gambling operator must ensure that they are also carried out at regular intervals.

This requirement cannot be bypassed, and the gambling operator must determine appropriate review intervals on a risk-based basis. This means that intervals can be determined on the basis of an individual customer's risk assessment, and customers can be categorised into different risk groups (e.g. low, normal or high risk) based on their gambling behaviour, gambling expenditure and related activities. Separate review intervals can be set for each group, for example one for normal-risk customers and another for high-risk customers.

Risk assessment must not result in customer due diligence procedures not being carried out at all.

In accordance with the risk-based approach, gambling operators must focus their resources particularly on those customer relationships where the risk is higher. Low-risk customers do not necessarily require such frequent monitoring. The scope of customer due diligence procedures is determined on the basis of a risk assessment of the customer relationship.

Legislation does not set requirements for how the know-your-customer procedure is carried out, so it can be either an automated or a manual process. A gambling operator's process requirements depend on the size of the company, which means that larger gambling operators have more extensive obligations.

6.3.4 Transactions exceeding a certain threshold

Under the Money Laundering Act, a gambling operator must carry out customer due diligence measures if the stake placed by the customer, the winnings cashed out, or both, amount to at least €2,000 in a single transaction or in linked transactions. This means that if, for example, a customer cashes out winnings of at least €2,000 or places a bet of at least €2,000 at a gambling operator's retail outlet, customer due diligence measures must be carried out. The threshold is also met, for example, in a situation where a customer cashes out two separate winnings whose combined total is at least €2,000. In this case, these are considered to be so-called linked transactions.

Interconnected transactions are not defined in greater detail in the Money Laundering Act, its preparatory materials or the Money Laundering Decree. For example, the temporal connection between linked transactions has not been clarified in the legislation. According to the supervisory authority's established view, transactions carried out by the same person on the same day are considered to be linked transactions.

The AMLA will issue guidance on linked transactions and their definition in July 2027. Following this, the supervisory authority's guidance will be updated and gambling operators will be informed of any changes and clarifications.

6.3.5 Suspicion of money laundering or terrorist financing

A gambling operator must carry out customer due diligence procedures whenever it has information or a suspicion of money laundering or terrorist financing. This requirement also applies to situations where the stake, payout or both are less than €2,000.

If a customer refuses to provide the information required to carry out customer due diligence measures, the gambling operator must report the matter to the Financial Intelligence Unit and provide it with the information in its possession. Further information on making a report is provided in Chapter 7 of these guidelines.

6.3.6 Suspicious nature of previously obtained customer information

If a gambling operator has reason to doubt the accuracy or adequacy of customer information previously obtained, it must carry out customer due diligence procedures again.

The gambling operator must make a case-by-case assessment of what information needs to be obtained. Based on a risk assessment, the gambling operator must decide whether the entire customer identification procedure needs to be repeated or only certain parts of it. This also depends on whether the previous information is incomplete or incorrect.

6.3.7 Large, unusual and/or irrational deposits

Large, unusual and/or irrational deposits must be halted and verified before the customer can use them for gambling. The purpose of the verification is to ensure that the customer is the genuine holder of the bank account linked to the gambling account and that the deposits originate from legally obtained funds.

It is important that enhanced customer due diligence measures are not implemented too late in relation to the making of deposits. When a gambling operator detects suspicious activity, enhanced measures must be implemented without delay. This means that the measures must be taken at the time of the deposit, and not only when the customer wishes to withdraw funds from their gaming account.

If a customer is unable to confirm the origin of the deposit or refuses to provide information on the source of the funds, **it may** be appropriate to report the matter to the Financial Intelligence Unit. For more information on the Financial Intelligence Unit and reporting to it, see Chapter 7 of these guidelines.

6.4 Customer due diligence in relation to compliance with sanctions regulations and freezing orders

The reporting entity must, as part of the customer due diligence measures laid down in Chapter 3 of the Money Laundering Act, have effective operating principles, procedures and internal controls in place to ensure that the reporting entity complies with the obligations arising from:

1) the regulations adopted pursuant to Article 215 of the Treaty on the Functioning of the European Union and the Government Decrees referred to in Section 1 and Section 2a(1) of the Act on the Fulfilment of Certain Obligations of Finland as a Member of the United Nations and the European Union (659/1967) (sanctions regulation); and
2) decisions issued pursuant to Section 2b of the Act referred to in paragraph 1 and pursuant to the Act on the Freezing of Funds for the Purpose of Combating Terrorism (325/2013) (freezing decisions).

According to the government proposal (HE 323/2022 vp) that led to the amendment of the Money Laundering Act , effective operating principles, procedures and internal controls refer to measures which, when implemented, enable entities subject to reporting obligations to detect and prevent activities that contravene sanctions regulations and freezing decisions. These measures include, for example, customer identification and verification, the collection of customer information and the ongoing monitoring of the customer relationship, as well as the comparison of customer information with current sanctions regulations and freezing decisions and the freezing of assets specified therein. Effective operating principles, procedures and internal

When establishing their monitoring arrangements, entities subject to the reporting obligation could tailor them to take into account, amongst other things, the scope of their operations, their geographical reach, and the nature and scope of the products and services they offer.

At present, entities subject to the notification obligation must take into account international sanctions based on regulations adopted pursuant to Article 215 of the Treaty on the Functioning of the European Union and on the fulfilment of obligations under the Act on the Fulfilment of Obligations Incumbent upon Members of the United Nations and the European Union in Finland(659/1967) and the Government Decrees referred to in Section 1 and Section 2a(1) of that Act (sanctions regulation). In addition to these sanctions, the identified risks are, in practice, also comparable to the identified risks associated with freezing decisions referred to in Section 16 of Chapter 3 of the Money Laundering Act.

The sanctions administered by the US Office of Foreign Assets Control (OFAC) are binding on US entities or those operating in the US, but they do not, as such, bind European or non-US companies operating within the EU. A gambling operator operating in Finland may therefore decide independently whether or not to comply with these sanctions in its operations. The supervisory authority also recommends compliance with OFAC sanctions.

A gambling operator subject to the reporting obligation under the Money Laundering Act must take into account the sanctions laid down in Chapter 3, Section 16 of the Money Laundering Act as a whole, even though, in the case of natural persons who are customers of the gambling company, the sanctions in question will in practice almost always be financial sanctions rather than, for example, restrictions on diplomatic relations or similar measures. When monitoring sanctions, the reporting entity must use up-to-date sanctions lists, such as the European Commission’s consolidated list of persons, groups and entities subject to EU economic sanctions.

Only natural persons may be customers of a gambling company. A gambling company may only offer online gambling to persons who hold a Finnish personal identity number and are resident in Finland. This can be seen as having the effect of reducing the risk of coercion in Finnish gambling, so the risk of coercion in gambling operations is not currently considered very likely. At physical venues, games may also be offered to persons who do not have a permanent residence in Finland. Gambling operators must take this into account in their operations and risk assessments if they offer games for play at physical venues.

The consequences could be significant if the risk materialises, as this could involve both money laundering and the financing of terrorism. The most significant risks identified in relation to sanctions and freezing orders in the gambling sector are personal, system and customer-related risks.

The reform of the Money Laundering Act regarding sanctions regulations related to customer due diligence is relatively new, so operational shortcomings relating to staff competence and the systems required for operations are possible. Those responsible for supervising operations must be trained to understand the principles of international sanctions and must know how to act in the event of potential sanctions hits. This requires the reporting entity to have effective internal processes in place so that the legal requirement for effective operating principles, procedures and internal controls can be deemed to have been met.

In addition to enhancing staff competence, it is essential that the internal division of responsibilities within the reporting entity for the organisation of sanctions control is taken into account.

It is not justified to organise sanctions monitoring in such a way that it is the sole responsibility of a single person in a situation where the scale of the reporting entity's business is significant in terms of both the number of cases and turnover.

System risks can be seen as another significant risk in the enforcement of sanctions in the gambling sector. Effective sanctions monitoring requires efficient and up-to-date systems that are capable of processing data from sanctions lists and the reporting systems of entities subject to reporting obligations efficiently and reliably. To ensure that the systems can be relied upon in this regard, their functionality should be developed and tested regularly. The systems should enable effective sanctions monitoring when a new customer is registering with a reporting entity's system. Similarly, monitoring should be organised in such a way that continuous monitoring of customers can be carried out in a manner that identifies any registered customers on the exclusion list as close to real time as possible.

In the supervisory authority's view, in the context of gambling operations, sanctions monitoring for the continuous monitoring of customers would be considered real-time if the monitoring were carried out at least once a day.

6.5 Verification of the origin of funds

Verification of the source of funds is an important part of knowing your customer. When a new customer registers, the gambling operator must ascertain the source of the funds the player uses for gambling. Possible sources of funds may include, for example, salary income, benefits, savings, gambling winnings and so on. A source of funds verification must also be carried out during the customer relationship if necessary, for example due to arisen suspicion or a detected discrepancy.

Gambling operators must be vigilant regarding the verification of the origin of funds provided. The gambling operator must ensure that the verification provided is reliable, sufficient and consistent with other information provided by the customer. Gambling operators cannot rely **solely on net deposits or previous winnings** without separately verifying the origin of the funds. **Simply returning previous winnings to a gaming account does not automatically mean that the funds are lawful.**

To verify the source of funds, it is usually necessary **to check bank statements** so that the gambling operator can confirm, for example, that the funds in question are winnings paid out by the operator which the player is depositing back into their gaming account.

Examples of situations where the explanation provided regarding the origin of funds may not be sufficient or reliable:

- The customer stated in the identity verification questionnaire during registration that they are unemployed, but nevertheless states that the source of their funds is ‘salary income’
- The customer stated, for example, a monthly salary of €2,000 during registration, but states that they gamble or gamble with significant sums
- The customer makes large single bets, but these are inconsistent with their income
- The customer has stated that the source of their funds is “gaming winnings”, but the gambling operator is unable to verify this.

These examples are provided for guidance only and should not be regarded as exhaustive. The gambling operator must ensure that it has sufficient information about its customers to reliably compare the source of funds with other information provided and to assess the reliability of that information.

Source of funds reports form part of a gambling operator’s risk-based operations. The greater the risk involved (for example, large and rapid bets or inconsistencies in the information provided), the more thorough the measures required of the gambling operator. These measures may include updating customer due diligence procedures, contacting the customer directly, and obtaining more detailed information.

6.6 Inadequate customer due diligence

If a gambling operator is unable to carry out the measures prescribed in Chapter 3 of the Money Laundering Act to identify the customer, it may not establish a customer relationship, conduct a transaction or maintain a business relationship. A gambling operator may therefore not register as a customer a person who refuses or is unable to provide sufficient information to establish a customer relationship. In the case of an existing customer relationship, the gambling operator must suspend transactions and prevent the customer from gambling until sufficient information has been obtained. If necessary, the gambling operator must report the suspicious transaction to the Financial Intelligence Unit and terminate the customer’s account.

A gambling operator must not register as a customer a person whom it has previously terminated due to insufficient documentation. In such a situation, the customer may only be re-registered as a customer once they have provided sufficient clarification regarding the situation or suspicion that was previously under investigation.

7 Reporting to the Financial Intelligence Unit

7.1 General information about the Financial Intelligence Unit

The task of the Financial Intelligence Unit (FIU) is to act as Finland's Financial Intelligence Unit (FIU) and to form part of the National Bureau of Investigation's national intelligence operations. The Financial Intelligence Unit's task is to prevent, detect, investigate and bring to justice crimes and the financing of terrorism. The activities of the Financial Intelligence Unit are governed by the Act on the Financial Intelligence Unit.

The tasks of the Financial Intelligence Unit include, among other things:

- preventing, detecting and investigating money laundering and terrorist financing, and referring such cases for investigation
- receiving reports of suspicious transactions and terrorist financing, and providing feedback to those subject to the reporting obligation
- cooperation with parties subject to reporting obligations and the authorities
- conducting operational and strategic analyses.

The Financial Intelligence Unit receives reports of suspicious transactions from entities subject to reporting obligations, and processes, analyses and discloses relevant information to other authorities in Finland. There is also close international cooperation. The Financial Intelligence Unit has the right to obtain, use and disclose information.

7.2 Reporting a suspicious transaction

Under Chapter 4 of the Money Laundering Act, a gambling operator must examine and report suspicious transactions. Making a report does not require evidence that money laundering or terrorist financing has actually taken place. If the suspicions remain after closer scrutiny, the matter must be reported to the Financial Intelligence Unit without delay.

A suspicious transaction refers to gambling activity that deviates from the customer's usual behaviour or is atypical for their activities. It is therefore extremely important to be familiar with the customer's usual behaviour, as discussed earlier in these guidelines. It may be difficult or impossible for a gambling operator to identify suspicious transactions and behaviour that deviates from a customer's usual patterns if it does not know its customers and their usual behaviour sufficiently well.

If a gambling operator or its agent observes unusual gambling activity, they must investigate the reasons for the gambling. If the gambling still appears suspicious after the investigation, or if no explanation is provided at all, the matter must be reported to RAP without delay. If the observation of a suspicious transaction is made by a gambling operator's agent, the agent may report the matter to the gambling operator, in which case the gambling operator will make the report to RAP.

The goAML reporting system serves as the reporting channel to RAP.

Gambling operators must register with the reporting system before submitting a report. Gambling operators must also comply with the regulation issued by RAP regarding the format of reports on suspicious transactions and the layout of the content. **The regulation applies to all entities subject to the reporting obligation**. Gambling operators must familiarise themselves with the content of the regulation.

The correct technical format of the reports and the layout of the content are essential for the RAP to carry out its statutory duties. For this reason, entities subject to the reporting obligation are required to submit reports of suspicious transactions to RAP in the format specified in the regulation, and failure to comply with these requirements will result in the automatic rejection of the report in question. Depending on the extent and frequency of the non-compliance, failure to meet the requirements may result in the RAP being obliged to report the non-compliance to the competent supervisory authority.

Submitting a report to the RAP does not always directly require the termination of the business relationship. However, the report must result in the gambling operator reassessing the customer's risk and tightening the monitoring of the customer relationship. The gambling operator must therefore obtain sufficient information about the customer and always terminate the business relationship if it does not have sufficient information about the customer to manage the risk of money laundering or terrorist financing.

A suspicious purchase of gambling services or redemption of winnings must always be refused. A report of a suspicious transaction must also be made if a fact subsequently comes to light that makes the gambling activity suspicious. A report of a suspicious transaction must therefore be made regardless of whether the gambling transaction was accepted, suspended or refused.

Reports must be made with a low threshold. This is not a criminal report, and it is not the responsibility of the gambling operator or agent to assess whether there is sufficient evidence for the transaction.

The Money Laundering Act also contains provisions regarding confidentiality. A gambling operator must not disclose to a customer or to third parties that it has made, or is going to make, a report to the RAP.

RAP publishes an annual report in which it reviews reports of suspicious transactions made across various sectors during the year. The number of suspicious transaction reports to RAP has increased over the years across all sectors. The supervisory authority recommends that gambling operators monitor and familiarise themselves with RAP's annual reports.

7.3 Indicators of suspicious transactions in gambling operations

The Financial Intelligence Unit has compiled a list of money laundering indicators to which entities subject to the reporting obligation should pay attention in their operations. The purpose of the list is to assist those subject to reporting obligations in identifying money laundering and suspicious transactions, as well as in making reports concerning suspicious transactions.

The following factors may be indicators of money laundering or suspicious transactions in gambling operations:

- The customer uses a company account(s) or a minor's account for gambling.
- The customer deposits funds into a gaming account but does not play.
- The customer deposits funds into a gaming account, but the source account and the withdrawal account are different.
- The customer transfers funds back via the game to the same account from which the original transfer was made.
- The customer deposits large sums into their gaming account relative to their annual income.
- The customer loses disproportionately large sums each month compared to their annual income.
- The customer gambles or purchases chips for an amount that is not commensurate with their known financial position.
- The customer's gambling behaviour differs significantly from their previous gambling behaviour.
- The customer's gambling behaviour differs from that of the rest of the customer group.
- The customer has a history of payment defaults, yet their gambling volume is high.
- Third parties are involved in depositing and withdrawing funds at the casino.
- The customer requests that chips be paid out to a third party.
- The customer regularly purchases chips, apparently deliberately keeping the amount below the reporting threshold.
- The customer sells or purchases chips or deposits cash in disproportionately large amounts.

The list of indicators is not exhaustive, and conversely, behaviour consistent with the list is not always a sign of money laundering or other criminal activity. The aim of the list is to catalogue, by sector, the most common indicators from the RAP's perspective for those subject to reporting obligations, drawing on both national and international phenomena and observations in the field of money laundering.

8 Use of agents

Under the Money Laundering Act, a gambling operator may delegate the measures prescribed for customer due diligence to a third party provided certain conditions are met. However, the gambling operator must bear in mind that, in accordance with Section 7 of Chapter 3 of the Money Laundering Act, it remains responsible for all obligations under the Act. This means that the gambling operator is always liable for any breaches and/or failures to comply with the obligations under the Money Laundering Act by the agent.

At gaming outlets selling the gambling operator's games, the gambling operator must identify and take into account the risks associated with potential breaches of the obligations under the Money Laundering Act in the sale of gambling games. The gambling operator must ensure that those selling gambling games

have sufficient experience and knowledge of money laundering risks. Particular attention must be paid to ensuring that new employees have an adequate level of knowledge regarding the prevention of money laundering and the ability to detect suspicious transactions.

When operating gaming terminals, the gaming operator must comply with the mandatory identification requirements set out in Section 28 of the Gambling Act. Customers must always be identified before they are permitted to play games of chance. Furthermore, customer due diligence measures must be carried out in situations required by the Money Laundering Act (see Chapter 6 of these guidelines). In addition, persons selling gambling services must identify suspicious transactions and report them.

Through continuous and regular training, and by ensuring that up-to-date information is provided on, among other things, money laundering indicators, a gambling operator can reduce the risk of non-compliance with the obligations of the Money Laundering Act and, at the same time, enhance employees' skills and knowledge. Agents and other responsible employees must be trained to identify and detect suspicious transactions, linked transactions and instances where thresholds are exceeded. Only those individuals who have received appropriate training based on anti-money laundering legislation and risk assessments should be involved in the sale of gambling products. The gambling operator must ensure that persons selling gambling products understand the importance of reporting suspicious transactions in preventing money laundering and terrorist financing.

The EU Anti-Money Laundering Regulation introduces changes regarding the use and status of agents. In accordance with the Anti-Money Laundering Regulation, a gambling operator may outsource certain measures relating to money laundering and terrorist financing. An outsourcing agreement must be drawn up for such outsourcing. The gambling operator must ensure that the entity to which tasks are outsourced is familiar with the regulations of the Money Laundering Act and is capable of fulfilling anti-money laundering measures. Gambling operators must note that they are not relieved of their responsibilities under the Money Laundering Regulation, even if they outsource certain functions.

The Anti-Money Laundering Regulation will come into force in July 2027. The supervisory authority will issue more detailed guidance on outsourcing at a later date.

9 Training

Gambling operators have a statutory obligation to train their staff on the content of the Money Laundering Act. The purpose of the training is to ensure that employees understand the importance of preventing money laundering, recognise the risks and know how to act in accordance with the regulations.
Training forms part of the operator's overall obligation to prevent money laundering and maintain a trustworthy gaming environment.

The gambling operator must ensure that employees whose duties are relevant to the prevention of money laundering or terrorist financing receive ongoing appropriate training and information. The training must be up-to-date and comprehensive, and its content must be updated as legislation or operational risks change. The gambling operator must therefore ensure that its staff have up-to-date and sufficient knowledge of the content and obligations of the Money Laundering Act.

Training must ensure that staff have sufficient competence to comply with the gambling operator's routines and guidelines. The content of the training must be adapted in accordance with the employee's duties, responsibilities and the licence holder's general risk assessment.

Regular training provided to the gambling operator's staff must cover at least the following areas:

- Key provisions of the Money Laundering Act
- the duty to know your customer
- Identification of suspicious transactions
- Practical implementation of the reporting obligation
- procedures for dealing with suspicious situations.

The training requirement applies to all persons who:

- are involved in customer service or the processing of payment transactions
- supervise gaming operations
- are responsible for anti-money laundering activities (e.g. compliance or risk management duties)
- hold senior management positions within the company and decide on practical measures
- New employees must also be provided with training as part of their induction before commencing their duties.

The gambling operator must document:

- the content of the training
- training dates
- participants
- any training materials.

The documentation must be retained for at least five years and presented to the supervisory authority upon request.

Through the training, employees must:

- Recognise situations that may be linked to money laundering or the financing of terrorism.
- Understand their own duties and responsibilities in relation to the Money Laundering Act.
- Be able to act in a timely manner and in accordance with instructions, for example by making an internal report or halting a transaction where necessary.

Training may be delivered internally or with the assistance of an external expert. Online training is an acceptable format, provided that the quality of the content and traceability requirements are met. Training may utilise practical examples, case studies and tests to ensure competence.

Gambling operators have no statutory obligation to train their agents and gaming staff on the content and obligations of the Money Laundering Act. However, it is in the gambling operator's own interest to train agents and gaming vendors, as the gambling operator is always liable for any breaches or violations of the Money Laundering Act by an agent and/or gaming vendor. The supervisory authority may therefore impose supervisory measures or sanctions on a gambling operator due to a breach or violation of the Money Laundering Act by an agent or game vendor employed by the operator.

The supervisory authority recommends that gambling operators provide adequate and regular training on the key obligations under the Money Laundering Act to the agents and gaming vendors they employ.

10 Internal control and whistleblowing system

10.1 Internal control

Through its internal controls, a gambling operator must prevent money laundering and the financing of terrorism, ensure compliance with the Money Laundering Act and the regulations and provisions issued pursuant to it, ensure the appropriate handling of customer and business data, and protect employees who report suspicious transactions (see section 10.2 'Whistleblowing system').

The gambling operator must appoint a person or unit responsible for internal control. The role of the responsible person or unit is to supervise and coordinate anti-money laundering measures, maintain internal guidelines, and report to management and the authorities.

The task of internal control is to regularly assess the risks of money laundering and terrorist financing associated with business operations, define measures according to the risks (e.g. know-your-customer procedures, ongoing monitoring, enhanced supervision) and to document the risk assessments and the measures taken on the basis of them.

Internal control must draw up and keep up to date internal guidelines covering

- customer due diligence (KYC)
- the identification and assessment of unusual transactions
- the practical implementation of reporting obligations
- data processing, storage and confidentiality
- internal reporting channels and procedures for handling reports
- intra-group information exchange, where applicable.

A gambling operator's internal control procedures include an obligation to provide staff with regular training on anti-money laundering obligations. Further details on this training obligation can be found in Chapter 9 of these guidelines.

The gambling operator must, for example, assess the effectiveness of internal control through internal audits or other evaluation methods, rectify any shortcomings and update its own guidelines where necessary. The results of the monitoring and the measures taken must be documented.

The senior management of the gambling operator is responsible for ensuring that internal control is properly organised. Management must regularly monitor the effectiveness of internal control and respond to any shortcomings.

10.2 Whistleblowing system

In accordance with Section 8 of Chapter 7 of the Money Laundering Act, a gambling operator must have procedures in place whereby its employees or agents can report suspected breaches of the Money Laundering Act and the regulations and provisions issued pursuant to itwithin the gambling operator (the so-called whistleblowing system).
This means that employees and contractors have the opportunity to report internally if the gambling operator breaches anti-money laundering rules.

The gambling operator must ensure safe and effective whistleblower protection so that employees can raise concerns without fear of repercussions. These measures are a key part of the overall framework for combating money laundering and terrorist financing. It must be possible to make a report via a dedicated, independent and anonymous channel.

The aim of whistleblower protection is:

- encourage employees to report concerns raised in good faith without fear of reprisals
- protect the whistleblower from discrimination, retaliation or disciplinary action
- ensure that reports are handled confidentially and appropriately.

A gambling operator must:

- establish an internal reporting channel through which employees can make reports anonymously or confidentially
- appoint a body to receive and handle reports impartially and without delay
- ensure that the identity and details of the whistleblower are kept confidential
- document and retain reports in accordance with the law
- take the necessary measures if the report proves to be justified.

11 More on the prevention of money laundering and terrorist financing

The National Police Board also recommends consulting the following sources, which are referred to in these guidelines.

Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (‘the Anti-Money Laundering Regulation’).

Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on mechanisms to be implemented in Member States to prevent the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849 (“6th Anti-Money Laundering Directive”).

Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the European Union Anti-Money Laundering Authority and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 (“AMLA Regulation”).

Government proposal to Parliament to supplement the Government proposal (HE 236/2021 vp) on amending the Act on the Prevention of Money Laundering and Terrorist Financing and Sections 3 and 20b of the Act on Financial Supervision

INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION - The FATF Recommendations (updated 6/2025).

Act on the Prevention of Money Laundering and Terrorist Financing | 444/2017 | Finnish Statute Book | Finlex

Act on the Financial Intelligence Unit (445/2017)

Act amending Section 1 of the Act on the Freezing of Funds for the Purpose of Combating Terrorism | 1162/2013 | Statutes of Finland | Finlex

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the
(SNRA, 2022)

SNRA 2022 Annexes REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities

National Police Board’s supervisor-specific risk assessment on the prevention of money laundering and terrorist financing (2024). Prevention of money laundering and terrorist financing in gambling operations - Poliisi.fi

Moneylaundering.fi

Financial Intelligence Unit (2021). Money laundering indicators.

Financial Intelligence Unit (2025). Regulation on the form of reports concerning suspicious transactions and the layout of their content.

Financial Intelligence Unit (2025). Financial Intelligence Unit Annual Report 2024.

Ministry of Finance Publications – 2021:17. National Risk Assessment on Money Laundering and Terrorist Financing 2021.

Annex to the National Risk Assessment on Money Laundering and Terrorist Financing 2021: Action Plan for the National Risk Assessment on Money Laundering and Terrorist Financing 2021–2023

Ministry of Finance Publications – 2024:8. National Risk Assessment on Money Laundering and Terrorist Financing 2023: Partial Update.

Annex to the National Risk Assessment on Money Laundering and Terrorist Financing 2023: Action Plan for the National Risk Assessment on Money Laundering and Terrorist Financing 2024–2025

National Police Board, Lottery Administration
Konepajankatu 2, PO Box 50, 11101 Riihimäki
Telephone +358 295 480 181, poliisi.fi