Written guidelines for obliged entities on the prevention of money laundering and terrorist financing in gambling activities

Contents

Definitions

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

Anti-Money Laundering Authority (AMLA) - The EU Authority for Anti-Money Laundering

Politically Exposed Person (PEP) – a politically influential person

VAS - a statement of the source of funds

Suspicious Transaction Report (STR)

Financial Intelligence Unit (FIU)

Supranational Risk Assessment (SNRA)

National Risk Assessment (NRA)

1 Introduction

1.1 Intent and objective of the guidelines

These guidelines are intended for gambling operators licensed in Finland, their employees, and other relevant stakeholders. The content of these guidelines is relevant to all gambling operators that apply for or hold a licence. It is also useful for their representatives.

These guidelines are not a detailed manual on how individual gambling operators should operate. However, they provide an overview and summary of a gambling operator's obligations with respect to the key provisions of the anti-money laundering regulations. They also outline possible approaches to risk-based practices and provide examples of effective measures to prevent money laundering and terrorist financing.

The user of these guidelines must always assess whether they are applicable to each specific case. In addition, gambling operators must always take into account the provisions of the Act on Preventing Money Laundering and Terrorist Financing, the orders of the supervisory authority, and general guidelines on the prevention of money laundering and terrorist financing. Gambling operators must also take into account the regulator-specific risk assessment, the National Risk Assessment (NRA), and the Supranational Risk Assessment (SNRA) in their operations.

The supervisory authority publishes the latest information, such as its risk assessment and updated guidelines on the prevention of money laundering and terrorist financing, in its own channels. The supervisory authority also announces changes in national and supranational risk assessments. Gambling operators should actively monitor the

supervisory authority's communications. In addition, the supervisory authority advises gambling operators to actively monitor the rahanpesu.fi website. The website provides the latest information on the prevention of money laundering and terrorist financing in Finland.

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

The Finnish gambling market is undergoing major changes, as the new Gambling Act (10/2026) will make gambling a partially licensed activity. Applications for an exclusive licence and a gambling licence (hereinafter referred to as a "licence") under the Gambling Act may be submitted from 1 March 2026, and operations may commence on 1 July 2027. The National Police Board's Gambling Administration will serve as the supervisory authority until 30 June 2027, and the Supervisory Agency will take over as the supervisory authority on 1 July 2027.

Gambling operators are obliged entities as referred to in the Anti-Money Laundering Act (the Act on the Prevention of Money Laundering and Terrorist Financing, 444/2017). The relevant provisions of the Anti-Money Laundering Act also apply to a business operator or entity that transmits participation notifications or payments in the meaning of chapter 1, section 2, subsection 1, points 9 and 10 of the Act, if the gambling operator has delegated the task of customer identification and notification to another business operator or entity.

It should be noted in this context that a comprehensive reform of the national anti-money laundering legislation was underway when these guidelines were written. The comprehensive reform will implement the EU's 6th Anti-Money Laundering Directive. The new Anti-Money Laundering Act will largely take effect on 10 July 2027, when the EU Anti-Money Laundering Regulation will also come into force. The new Anti-Money Laundering Act and the Anti-Money Laundering Regulation introduce changes to the obligations of obliged entities. **These guidelines have been drafted in light of current anti-money laundering legislation, and the supervisory authority will issue new guidelines when the new act and the Anti-Money Laundering Regulation come into effect.**

The Anti-Money Laundering Act seeks to prevent money laundering and terrorist financing, facilitate the detection and investigation of such activities, and improve the tracing and recovery of the proceeds of crime. The primary objective of anti-money laundering regulations is to prevent business activities from being used to launder money and finance terrorism. At the same time, it is essential to ensure that there are no unnecessary restrictions on the conduct of efficient business operations. Balancing these interests requires the licenceholder to take a **risk-based approach**.

The risk-based approach must permeate all of the gambling operator's work to prevent money laundering and terrorist financing. In other words, the measures must be proportionate to the risks associated with the operator's activities. The risk-based

regulation of the Anti-Money Laundering Act enables gambling operators to effectively focus their efforts on the areas with the greatest risk of money laundering and terrorist financing.

A risk-based approach requires gambling operators to have a thorough understanding of the risks associated with money laundering and terrorist financing, particularly in the gambling sector, and be capable of making informed decisions. This, in turn, requires the development of expertise through, for example, training, guidance, professional advice, and practical experience.

The Anti-Money Laundering Act requires gambling companies to take active measures to prevent money laundering and terrorist financing. This obligation includes, among other things, actively monitoring customers, identifying suspicious transactions, and reporting them to the authorities. Violating or failing to comply with the obligations under the Anti-Money Laundering Act may result in penalties, such as administrative sanctions, revocation of the licence, or criminal prosecution.

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)**, mainly due to large bets, large amounts of winnings, high turnover, and the use of cash. Money launderers often accept potential losses, which means that a person may lose significant sums of money, while any potential gains can be made to appear as legitimate income. For these reasons and others, gambling can be an attractive means of money laundering for criminals. See Chapter 4 for more information on the national risk assessment.

Given the moderately significant risk, it is important that gambling operators have adequate practices in place to combat money laundering and terrorist financing practices in light of the nature and scope of their operations.

The importance of complying with the obligations under the Anti-Money Laundering Act is underscored by the fact that the supervisory authority can impose an administrative penalty, a fixed penalty, or a public warning on a gambling operator as an administrative sanction for neglecting or violating its obligations under the Anti-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 more than 200 countries and jurisdictions. They are committed to having their efforts to combat money laundering, terrorist financing, and the financing of 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 to prevent and combat money laundering and terrorist financing. As a member state, Finland is required to comply with the FATF recommendations.

The provisions of the Anti-Money Laundering Act are largely based on the EU Anti-Money Laundering Regulation and EU Anti-Money Laundering Directives, which in turn are based on the FATF's recommendations.

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

Finland, along with other EU countries, is facing changes to anti-money laundering regulations. The Member States adopted a new legislative package on 31 May 2024. It aims to establish a more detailed and consistent regulatory framework. Among other things, the legislative package means that a large part of Anti-Money Laundering Directive 4 will be replaced by the Anti-Money Laundering Regulation, which is directly binding and directly applicable in the Member States. The Anti-Money Laundering Regulation will take effect on 10 July 2027.

The provisions of the 4th Anti-Money Laundering Directive that were not incorporated into the regulation have been replaced by the 6th Anti-Money Laundering Directive. The provisions of the 6th Anti-Money Laundering Directive will be incorporated into national anti-money laundering legislation and will take effect on 10 July 2027.

2.3 AMLA Regulation

In addition to the EU's anti-money laundering package, a new authority—the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA)—has been established at the EU level under the AMLA Regulation. AMLA was officially established in July 2024 and began operating in 2025. It is based in Frankfurt, Germany. Most of the authority's functions will begin in 2025 and 2026, except for the direct supervision of obliged entities in the financial sector and certain functions related to sectors other than the financial sector, which will begin in 2028.

As financial crime is international in nature, the new authority will enhance the effectiveness of the system to prevent money laundering and terrorist financing by establishing, in coordination with national supervisory authorities, a mechanism to ensure that obliged entities comply with their obligations on the prevention of money laundering and terrorist financing in the financial sector. AMLA is also tasked with supporting sectors outside the financial industry and coordinating the financial intelligence units of member countries.

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

2.4 National legislation

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

When these guidelines were written, a comprehensive reform of the national anti-money laundering law was underway to implement the 6th EU Anti-Money Laundering Directive. The comprehensive reform will bring about significant changes to Finnish legislation.

In addition to national law, the EU Anti-Money Laundering Regulation is directly applicable in Finland. Most of the Anti-Money Laundering Regulation will take effect 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 when they take effect.

3 Money laundering and terrorist financing

3.1 What is money laundering?

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

The definition of money laundering is set out in chapter 1, section 4 of the Anti-Money Laundering Act, which states that money laundering refers to the activities described in chapter 32, sections 6–10 of the Criminal Code (39/1889).

In money laundering:

- The funds are of illicit origin.
- The aim is to channel the funds through the legitimate 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 channelled through the legitimate payment system in order to conceal or obscure the true nature, origin, or ownership of those funds. Money laundering therefore requires a predicate offence. A predicate offence can be any act punishable by law that has resulted in financial gain for the perpetrator.

Receiving, using, converting, handing over, transferring, brokering or possessing criminal funds are also forms of money laundering. The person must have the intent to launder money, meaning that they intend to obtain a benefit, assist a criminal, or conceal the illicit origin of the assets. Money laundering also involves concealing or disguising the true nature, origin, location, or disposition or rights to assets gained through criminal activity.

Money laundering is generally 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 that, attempts are made to obscure the illicit origin of the funds, for example through complex transactions. For example, the funds are moved through multiple accounts between several countries to take them further away from their source. Ultimately, the funds are brought back into the legitimate economy.

Preventing money laundering can also help prevent other crimes, as money launderers may use those funds to finance new crimes. Money laundering is often part of organised and international criminality. Money laundering can threaten the stability, reliability, and competitiveness of the financial system. Instability can drive up the costs of loans, payment transactions, and insurance, and the effects may be felt more broadly across the economy.

Money laundering methods vary and can range from simple to more complex. They do not only concern cash transactions. Money that is already in the financial system can also be vulnerable to money laundering.

3.2 What is terrorist financing?

According to chapter 1, section 4 of the Anti-Money Laundering Act, the financing of terrorism refers to the activities referred to in chapter 34a, sections 5, 5a and 5b of the Criminal Code. The financing of terrorism involves obtaining or collecting funds for terrorist activities. This is not just a question of donations. Terrorist financing also includes the collection, transfer and receipt of funds used for terrorism. Terrorism is often financed with legitimate funds, which makes it particularly difficult to detect.

In terrorist financing:

- The funds may be of legal or illegal origin.
- The funds are obtained 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 collecting, transferring and using funds. Terrorism is primarily financed with funds obtained from legitimate sources, and financial transactions take place via bank transfers, cash or money transfer services. Financial transactions take place between several different countries.

To combat terrorism and prevent the financing of terrorism, a natural person or legal entity may have their funds frozen in accordance with the provisions of the Act on the Freezing of Funds with a View to Combating Terrorism (325/2013). Assets can be frozen to prevent the person who possesses them from channelling the funds for terrorist purposes. In Finland, the National Bureau of Investigation issues asset freezing orders and maintains a public register of such orders. The freezing order is enforced by the National Enforcement Authority Finland.

Sanctions are also imposed to combat terrorism and prevent terrorist financing. Their practical effect is to restrict economic or other cooperation with designated entities. Sanctions are intended to influence activities that are considered a security threat, for example. Financial sanctions such as asset freezes may be used in the fight against terrorism. The Ministry of Foreign Affairs lists the sanctions against terrorism on its website.

4 National and supranational risk assessments and the regulator-specific risk assessment

National and supranational risk assessments have been published on the prevention of money laundering and terrorist financing, and these are updated regularly. The supervisory authority has also published a regulator-specific risk assessment. Gambling operators must familiarise themselves with the risk assessments and other published guidelines and manuals and incorporate them, as appropriate, into their own risk assessments, which they must prepare based on their business models. Chapter 5 of these guidelines provides more information on the risk assessment of a gambling operator.

4.1 National risk assessment

As part of its efforts 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 supranational risk assessment for the European Union prepared by the European Commission. Under chapter 2, section 1 of the Anti-Money Laundering Act, the Ministry of Finance and the Ministry of the Interior are responsible for preparing the national risk assessment. In addition, numerous different entities are involved in preparing the risk assessment, including national competent authorities, supervisors under the Anti-Money Laundering Act, authorities with a duty of diligence, and private-sector entities.

The National Risk Assessment of Money Laundering and Terrorist Financing 2021 was prepared under the coordination of the Ministry of Finance and the Ministry of the Interior. The risk assessment describes the threats, vulnerabilities, and risks associated with money laundering and terrorist financing across all obliged sectors, as well as in the operations of non-profit organisations (NPOs). In addition, the risk assessment examines the risks of money laundering and terrorist financing associated with the specific phenomena under consideration.

The national action plan on money laundering and terrorist financing 2021–2023 was drawn up in connection with the risk assessment. The action plan outlines the measures intended to mitigate the risks identified in the risk assessment. The risk assessment and action plan form a comprehensive framework that reflects Finland’s national understanding of the risks of money laundering and terrorist financing and the measures required to manage them.

A partial update to the National Risk Assessment of Money Laundering and Terrorist Financing was prepared in 2023 under the coordination of the Ministry of Finance and the Ministry of the Interior. The update describes the threats, vulnerabilities and risks related to money laundering and terrorist financing in the sectors subject to the highest-risk obliged entities. In addition, the partial update to the risk assessment examines the risks of money laundering and terrorist financing in relation to selected phenomena. The update supplements the 2021 risk assessment; it does not replace it.

When the risk assessment was partially updated, the national action plan on money laundering and terrorist financing was updated for 2024–2025. The action plan outlines the measures intended to mitigate the risks identified in the risk assessment. The risk assessment and action plan form a comprehensive framework that reflects Finland's national understanding of the risks of money laundering and terrorist financing and the measures required to manage them.

The national risk assessment will be comprehensively updated in 2025–2026. The new national risk assessment is due to be published in early 2026. The supervisory authority will notify gambling operators of the content of the national risk assessment and any changes to it.

4.2 Supranational risk assessment

Article 6 of the Fourth Anti-Money Laundering Directive required the European Commission to prepare an assessment of the risks affecting the European Union's internal market due to money laundering and terrorist financing associated with cross-border transactions. This risk assessment is referred to as a Supranational 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 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 are associated with cross-border activities at the EU level. The risk assessment covers the key risks to the single market across a range of sectors, as well as horizontal vulnerabilities that may affect these sectors.

Based on this, the document sets out guidelines on risk-mitigation measures to be followed at the EU and national levels. In addition, it includes recommendations for various stakeholders and authorities.

4.3 Regulator-specific risk assessment

Under chapter 2, section 2 of the Anti-Money Laundering Act, the competent supervisory authority must prepare a risk assessment of the risks of money laundering and terrorist financing associated with the obliged entities under its supervision.

The regulator-specific risk assessment serves several purposes and objectives, all of which contribute to preventing money laundering and terrorist financing in the gambling sector. The aim is to identify and assess risks, evaluate their likelihood and impact, and present methods for managing the risks of money laundering and terrorist financing in the gambling sector. The purpose of the risk assessment is to identify and evaluate the money laundering risks associated with gambling.

It is impossible to identify all risks, but the goal is to identify the most likely and significant money laundering risks associated with gambling. A further purpose of the risk assessment is to propose some measures for reducing risks. For this reason, the risk assessment analyses the risks and presents means for controlling risk. The risk assessment evaluates the likelihood, impact and severity of the identified risks.

Risk assessment is a tool used in regulatory activities. It enables the supervision of the prevention of money laundering and terrorist financing to focus on activities where the risks are found to be the most significant. In the context of regulatory activities, this type of targeted oversight is referred to as risk-based supervision. On the other hand, identifying and assessing smaller risks is also important for gaining an overview and understanding of the comprehensive risks of money laundering and terrorist financing associated with gambling.

The risk assessment is the supervisory authority's assessment of the factors and events that pose a threat to gambling operations in terms of money laundering and terrorist financing. The risk assessment is also a tool for gambling operators. Among other things, gambling operators can compare the regulator-specific risk assessment with their own risk assessment of their operations and evaluate whether their gambling activities have taken into account all the risks identified in the regulator's risk assessment. They can also see how the regulator views the risks and the control measures.

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

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

Gambling operators should note that the regulator-specific risk assessment is a separate document from these written guidelines.

5 Obliged entity's risk assessment and risk-based approach

5.1 Obliged entity's risk assessment and risk management methods

The Anti-Money Laundering Act requires gambling operators to take risk-based measures to prevent their business from being misused 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 highest in their

business operations. The 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 modifies its business model, which could result in either an increase or a decrease in risk.

In order to implement a risk-based approach, the gambling operator must, therefore, conduct a risk assessment of its own business operations. The risk assessment is a key component of all other efforts to prevent money laundering and terrorist financing. It should serve as the basis for business practices and other measures to prevent money laundering and the financing of terrorism. 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 the likelihood of this occurring. **The risk assessment must consider all factors that could affect the risks of money laundering and terrorist financing**. In particular, the gambling operator must take into account the type of products and services offered, its customers, transactions, distribution channels, and geographical risk factors.

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

The 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 the applicable legislation. The gambling operator must also review its risk assessment if changes occur in the national or supranational risk assessments or the regulator-specific risk assessment that could affect the operator's inherent risk.

This requires the gambling operator to understand the actual risks and vulnerabilities. Therefore, the business must have expertise in money laundering and terrorist financing in the Finnish context. This is a fundamental factor in the effective implementation of a risk-based approach and requires gambling operators to continuously monitor the latest reports on money laundering and terrorist financing.

When conducting a risk assessment, the gambling operator must take into account the nature, size and scope of its operations. In light of the above factors, the 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 the following:

1) The development of internal policies, procedures, and controls
2) An internal audit, if this is justified given the nature and scope of the obliged entity's operations.

A gambling operator must establish the aforementioned policies, procedures and controls, and monitor and improve the related measures. If the obliged gambling operator is a legal entity, the board of directors, a general partner or another member of senior management in a comparable position must approve the policies, procedures and controls referred to in chapter 2, section 3, subsection 2 of the Anti-Money Laundering Act, and monitor and develop the related measures.

The gambling operator's risk assessment for the prevention of money laundering and terrorist financing must be a separate and independent document. Therefore, gambling operators should note that it is not sufficient to simply include anti-money laundering measures in a general risk assessment or, for example, a self-monitoring plan under section 35 of the new Gambling Act. The risk assessment and any amendments to it 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 procedures in place to combat money laundering and terrorist financing. The purpose of risk management methods is to prevent the identified risks from materialising in the operations. That is why it is important for the gambling operator to closely link its overall anti-money laundering risk assessment with the risk management methods.

Risk management methods must cover at least the following areas:

- Customer due diligence
- Monitoring and reporting
- Processing personal data
- Personnel suitability assessment and training
- Compliance with regulations and internal control

In addition to the 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 likelihood that money laundering or terrorist financing will occur, 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 oversight (vulnerability), and criminals seek to exploit this (threat), the risk is high.

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

A threat could be, for example:

- A criminal person or criminal 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 one.

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.

Examples of vulnerabilities include:

- Insufficient customer due diligence
- Ineffective or inadequate oversight
- Slow response to suspicious transactions
- Products that allow users to easily transfer money without any actual gaming purpose

5.2 Identification and assessment of risk factors

When assessing the risks associated with its business model, a gambling operator must identify and evaluate 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 components: the identification of risk factors and their evaluation.

A gambling operator must identify all material risk factors associated with its business model. In order for a gambling operator to identify the key risk factors that may affect its risk of being exploited for money laundering and terrorist financing, it must first conduct a thorough analysis of its business model and understand the vulnerabilities of its gambling services from 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, as well as how it has chosen to organise its business model.

When a gambling operator identifies risk factors associated with its business model, it must consider the national and supranational risk assessments and other relevant sources. It can be challenging to identify which specific features of a business model may pose a risk in terms of money laundering and terrorist financing. In this context, the purpose of national and supranational risk assessments is to help gambling operators obtain information on sector-specific risk factors. Similarly, other relevant sources, such as these guidelines and the regulator-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 take a comprehensive approach to assessing the extent to which the identified risk factors may expose it to money laundering and terrorist financing. A gambling operator may choose how to present its assessment of inherent risk factors. Risk factors can 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 occurring, as well as its potential consequences.

The gambling operator must conduct the assessment in a way that enables it to use the risk assessment as an operational tool to understand the areas and scopes to which it may be exposed to money laundering and terrorist financing. This allows the gambling operator to target its mitigation measures at the areas of highest risk.

As mentioned earlier, a gambling operator must assess the risk associated with each inherent risk factor in its business model separately. Simply assessing the overall risk level, which may be linked to several risk factors, is not sufficient. By assessing the risk separately for each individual risk factor, a gambling operator can better determine 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

The gambling operator’s risk assessment must cover, at a minimum, the risk factors associated with its customers, products and services, transactions, distribution channels, and geographic areas.

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

The scope of the risk assessment depends on the specific business model of the gambling operator. If a gambling operator has a broad business model — for example, one that offers a wide variety of gambling games both online and at brick-and-mortar locations — this places greater demands on the content and scope of risk assessments. In such cases, the gambling operator’s business model involves several risk factors that it must take into account in its efforts to combat 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 a gambling operator’s size and the scope of its operations, it must conduct a thorough analysis of how its specific business model may be vulnerable to money laundering and terrorist financing in the Finnish context.

5.3.1 Customer risk classification

Customer risk classification must be based on a general risk assessment of the business and the information the gambling operator has obtained 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, the **measures must be proportionate to the risks**. For example, verifying a customer's annual income or occupation may be sufficient for standard-risk customers, whereas in high-risk cases, additional verification and direct contact with the customer are required to determine the source of funds.

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

A gambling operator's specific business model determines which types of customers it must assess. Under section 21 of the Gambling Act, a gambling operator in Finland may offer electronic gambling and may only register customers who are natural persons with a permanent address in mainland Finland. However, the gambling operator must be aware that even if it only accepts customers from Finland, foreign customers may still attempt to circumvent the operator's restrictive measures, for example, by using false documents or VPNs.

When the new Gambling Act takes effect, it will no longer be necessary for customers to have a permanent address in mainland Finland in order to use gambling services at physical locations, such as through agents. Gambling operators must also take into account the risks that may arise from such customer relationships in their risk assessments and customer risk classifications. Gambling operators must also note that the requirement for customer identification applies to gaming at physical locations as well. Anonymous gambling is not permitted.

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

Once a gambling operator has identified all the relevant customer types, it must assess the risk posed by each customer group in terms of their potential to misuse the company for money laundering and terrorist financing. The gambling operator may include general information and experiences regarding the customers in its assessment. By analysing its customers, the gambling operator can gain an overview of the types of customers it has and determine whether the general behaviour of these customers affects the extent to which a particular customer group poses an inherent risk of the gambling company being exploited for money laundering and terrorist financing.

The gambling operator must continuously monitor each customer's risk classification and adjust the risk level as necessary. If a customer's risk is assessed to have risen since the business relationship began, the gambling operator must obtain additional information about the customer and, if necessary, intensify the ongoing monitoring and control. If a customer is assessed as posing a lower risk, monitoring and control do not need to be as comprehensive or take place as frequently.

The gambling operator's customer risk assessment must always include, at a minimum, the measures required for customer due diligence and PEP and sanctions screening. The gambling operator must obtain information about the purpose and nature of the business relationship, regardless of the customer's risk category. This information should also be reviewed on an ongoing basis. For example, a gambling operator may obtain information about a customer's annual income or whether the bank account associated with the customer relationship is a personal one. In addition, the source of the funds used for gambling must be identified. "Source of funds" refers to detailed information about a customer's financial situation and the origin of the funds deposited into their gambling account and used for gambling. Chapter 6 of this guide provides more information on customer due diligence measures.

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

5.3.2 Products and services

A 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 forms of gambling are equally susceptible to abuse. Certain types of games pose a markedly greater risk than others. Gambling operators must identify these high-risk game types and take them into account in their risk assessments, customer monitoring, and reporting practices. They may need to impose stricter identification and gaming restrictions on them.

Gambling is particularly susceptible to money laundering when it involves elements such as the following:

- The ability to make large one-off bets
- Fast-paced games with a high completion speed
- The chance to play against other people
- The ability to make moves within a game that intentionally benefit another player
- Using multiple accounts or third parties
- Insufficient oversight of player behaviour or financial transactions
- Use of cash
- If a gambling product is not based entirely on chance but includes elements such as skill

The following gambling activities have become particularly well-established as high-risk: **sports betting, poker and casino games.**

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

The gambling operator must identify and assess the risk factors for all of its gambling products. If a gambling operator offers several different versions of the same gambling product, these versions must be assessed separately if they differ significantly from the operator's other products. If the gambling operator's products differ only in cosmetics, a separate risk assessment is not required.

5.3.3 Transactions

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

For example, the gambling operator must consider that a payment method can be a suitable means of concealing the source of funds. Gambling operators must also consider the extent to which a payment solution can be misused by another person, and how easily this can occur. The gambling operator must also determine whether the payment solution allows for fast and large transactions.

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

The gambling operator must generally assess the risks associated with all the payment solutions it uses. If a gambling operator uses several different types of e-wallets or bank cards that all share the same general characteristics and are otherwise similar, the operator is not required to assess the risks separately for each payment method variant. In such cases, it is sufficient for the gambling operator to assess the overall risk of the entire payment method.

Gambling operators that offer multiple deposit and withdrawal options must be particularly vigilant about the possibility of funds being transferred to different accounts. One way to reduce the risks of money laundering and terrorist financing is **to only allow customers to withdraw money into the bank account from which the deposit was originally made**. This allows the gambling operator to ensure that the customer's financial activities remain consistent, as well as to manage and mitigate risks. However, gambling operators should note that on its own, the above procedure does not guarantee that the funds deposited into a gambling account are legitimately obtained. Gambling operators cannot rely solely on online deposits or previous winnings without separately verifying the source of the funds. **Simply crediting previous winnings back to a gambling account does not automatically mean that the funds are legitimate**.

5.3.4 Delivery channels

A gambling operator must identify and assess the risks associated with the delivery channels it uses. The gambling operator must, therefore, conduct a risk assessment regarding how it chooses to make its gambling products available to customers and how the gambling company interacts with customers in other ways.

This could mean, for example, that the gambling operator makes its gaming products available online or that it sells its gaming products in person at a physical 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 accessible via a gaming account or self-service terminals.

Regardless of a gambling operator's business model, it must assess the extent to which its distribution channels could be exploited for money laundering and terrorist financing.

5.3.5 Countries and geographical regions

The gambling operator must identify and assess the risks associated with countries and geographic regions. Geographical risks must be taken into account when classifying the gambling operator's customers, 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 in terms of money laundering and terrorist financing.

The gambling operator must take into account the risks associated with specific countries and geographic regions when selecting where it provides its gambling services. The gambling operator's assessment must consider whether there are strategic shortcomings in the country in relation to the prevention of money laundering and terrorist financing. In this context, it is important to determine whether the country is on the European Commission's list of high-risk third countries or on the FATF's grey and black lists. Gambling operators must not select destinations from countries on the FATF's grey or black lists.

6 Customer due diligence

6.1 General information about customer due diligence and risk-based assessment

Sufficient customer due diligence is essential for preventing and combating money laundering and terrorist financing. At present, the provisions on customer due diligence are mainly laid down in chapter 3 of the Anti-Money Laundering Act.

The basic requirement of the Anti-Money Laundering Act is that gambling operators must know their customers. This applies to all gambling operators. The purpose of customer due diligence is to ensure that the gambling operator knows who its customers are and why they have established customer relationships with the operator.

If a gambling operator is unable to carry out the customer due diligence measures prescribed in chapter 3 of the Anti-Money Laundering Act, it must not establish a customer relationship, conduct a transaction, or maintain a business relationship. The customer due diligence measures set forth in chapter 3 of the Anti-Money Laundering Act must be followed throughout the entire customer relationship, based on a risk-based assessment.

Customer due diligence is an important step in the gambling operator's understanding of the customer's typical behaviour, enabling it to identify unusual behaviour and changes in the customer relationship. A gambling operator must take action if it notices changes in a customer relationship, such as a change in the customer's gambling behaviour or gambling volume. A gambling operator must establish procedures to detect and respond to signs of money laundering or terrorist financing.

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

- When a customer registers
- When the customer's circumstances change
- Regularly throughout the customer relationship
- When a customer's bet and/or payout is 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 suspicions 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 a product or business relationship is, the more comprehensive the measures required to know the customer and prevent money laundering.

6.2 Due diligence procedures

6.2.1 Standard customer due diligence procedures

To comply with the customer due diligence requirements, obliged entities must take all of the following measures:

- Identify the customer and verify their identity
- Assess and understand the purpose and intended nature of the business relationship or individual transactions, and obtain relevant information where necessary
- Verify whether the customer has had targeted economic sanctions imposed on them
- Assess the nature of the customer’s business, work or profession, and obtain relevant information as necessary
- Continuously monitor the business relationship, including verifying transactions throughout the duration of the relationship to ensure that they are consistent with the information held by the obliged entity regarding the customer, the customer’s business activities and the risk profile, as well as, where necessary, the source of funds
- Determine whether a customer is a politically exposed person (PEP), a family member of such a person, or a person known to be a close business associate of such a person.

6.2.2 Enhanced due diligence obligation

Chapter 3, section 10 of the Anti-Money Laundering Act provides for enhanced customer due diligence. In some circumstances, standard customer due diligence measures are not sufficient, and enhanced due diligence measures are required. Enhanced due diligence requires the gambling operator to take more thorough measures than usual to verify a customer’s identity, business activities, and the source of their funds. Enhanced due diligence measures must be taken when a customer, transaction or service involves a higher-than-normal risk of money laundering or terrorist financing.

Enhanced customer due diligence measures should be taken in the following situations:

- The customer is a politically exposed person (PEP) or a close associate of such a person.
- The customer's operations are located in a high-risk country.
- The customer engages in unusually complex or abnormal transactions.
- The customer is not physically present during the identification process (e.g., remote transactions without reliable identification).

An enhanced due diligence requirement may include measures such as the following:

- A more in-depth analysis of the customer's background.
- A more detailed investigation into the identity or structure of a legal entity and its beneficiaries.
- Verification of political affiliations.

Assessment of the source of funds:

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

Clarifying the purpose and nature of the transaction:

- Why is the customer gambling (e.g., for entertainment or professionally)?

Continuous monitoring of operations:

- Continuous monitoring of customers' gambling activity and service usage to detect anomalies.

Management approval to establish or continue a customer relationship:

- For example, if the customer is a PEP, the management may have to decide whether to approve the customer relationship.

6.3 When should customer due diligence be carried out?

6.3.1 At the start of a customer relationship

A gambling operator must identify new customers and verify their identity using a reliable and independent source. In addition to the identification and verification requirements of the Anti-Money Laundering Act, section 20 of the Gambling Act also requires players to verify their identity when registering.

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

When a customer registers, the gambling operator must collect information regarding the purpose and nature of the business relationship. The gambling operator must determine whether the purpose of the customer’s business relationship is gambling for entertainment or professional gambling. The gambling operator must also determine how the customer intends to use the gambling products or services. By analysing the expected gambling behaviour, the gambling operator can assess the frequency of a customer’s transactions and the amount of their deposits.

Gambling operators must pay attention to the deposit limits set by customers when they gamble online. If a customer indicates from the outset that they gamble frequently and for large sums, the gambling operator may need to investigate further whether the purpose of the gambling is truly for entertainment. This requires additional checks and verification of customer information.

Gambling operators should ask questions during the registration process for new customers in order to know their customers better from the outset. The questions should

focus on determining the source and amount of future deposits, as well as the intended use of the funds. This information helps gambling operators gain a better understanding of the purpose and nature of the business relationship and facilitates control, monitoring and customer risk classification.

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

- What is the origin of the money you plan to use for gambling?
- What were your annual earnings last year?
- What do you do for a living?
- Where does your income come from?
- How often do you expect to play each month?
- What kinds of games do you normally 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 during the course of their relationship with the operator. This assessment is essential for enabling the gambling operator to detect deviations from the expected behaviour.

In addition to the above, the gambling operator must determine whether the customer is a politically exposed person (PEP) or a family member of a PEP. If the customer is a PEP, enhanced due diligence is always required. 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 customer relationships and material changes in circumstances

Chapter 3, section 4 of the Anti-Money Laundering Act requires a gambling operator to arrange monitoring that is adequate in view of the nature and extent of the customer's activities, the permanence and duration of the customer relationship and the risks involved in order to ensure that the customer's activities are consistent with the obliged entity's experience or knowledge of the customer and their activities. The gambling operator must therefore monitor **the customer relationship continuously throughout the relationship**. Customer information must be kept up to date, and the gambling operator must assess whether the transactions are consistent with the customer's risk profile.

The gambling operator must repeat the customer due diligence procedures if there is a material change in the circumstances of the customer relationship. An example of a material change in circumstances is if a customer becomes a politically exposed person (PEP) or if the customer's behaviour or gambling habits change significantly. An example of a change in a customer's gaming behaviour is when the customer starts playing in a different way or playing different games and betting larger amounts than before.

Based on the risk assessment, the gambling operator must determine whether the changed circumstances require the collection of new customer information, such as identification details or similar. The information to be collected depends on the situation. For example, it may be necessary to re-verify a customer's identity if a gambling operator learns that the customer has changed their name or personal identification number. In some cases, such as when there is a change in a customer's behaviour, simply verifying the customer's identity is not sufficient; instead, the gambling operator must also analyse the origin of the customer's funds and take other measures necessary to verify the customer's identity.

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. A customer does not need to be classified as high-risk in order for enhanced due diligence measures to be taken.

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

6.3.3 Regular due diligence during a customer relationship

Gambling operators are also required to take regular customer due diligence measures throughout the customer relationship. This is to ensure that the customer data held by the gambling operator is up to date and sufficient. In addition to conducting customer due diligence procedures whenever the customer's circumstances change substantially, a gambling operator must ensure that such procedures are also carried out regularly.

This requirement cannot be disregarded, and the gambling operator must determine appropriate audit intervals on a risk-based basis. This means that time limits can be set based on an individual customer's risk assessment, and customers can be categorised into different risk groups (such as low, normal or high risk) based on their gambling behaviour, expenditure, and related activities. Separate audit intervals can be set for each group; for example, there could be one for customers with normal risk and another for high-risk customers.

Risk assessment must not result in an absence of customer due diligence procedures.

In accordance with the risk-based approach, gambling operators must focus their resources on customer relationships where the risk is higher. For low-risk customers, frequent monitoring may not be necessary. The scope of customer due diligence procedures is determined based on the risk assessment of the customer relationship.

The law does not specify how the customer due diligence process must be conducted, so it can be either an automated or a manual process. The procedural requirements for gambling operators depend on the size of the company, which means that larger operators have more extensive obligations.

6.3.4 Transactions exceeding a certain threshold

Under the Anti-Money Laundering Act, a gambling operator must implement customer due diligence measures if a customer's bet, winnings, or both amount to at least €2,000 in a single transaction or in interconnected 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 an agent's premises on behalf of the gambling operator, customer due diligence measures must be taken. The threshold is also reached, for example, when a customer cashes out two separate winning bets with a combined total of at least €2,000. This is an example of an interconnected transaction.

The Anti-Money Laundering Act, the preparatory work for the Act, and the Anti-Money Laundering Regulation do not define interconnected transactions in any more depth. For example, the legislation does not clarify how far apart the transactions may be in time. In the supervisory authority's established view, withdrawals and/or deposits by the same person within a single day are considered interconnected transactions.

AMLA will issue guidance on interconnected transactions and their definition in July 2027. After this, the supervisory authority will update its guidelines, and gambling operators will be notified of any changes or clarifications.

6.3.5 If there is any suspicion of money laundering or terrorist financing

A gambling operator must carry out customer due diligence whenever it has information or suspicions regarding money laundering or terrorist financing. This requirement also applies when a bet, payout, or both are less than €2,000.

If a customer refuses to provide the information required for customer due diligence, the gambling operator must report the matter to the Financial Intelligence Unit and provide the information in its possession. Chapter 7 provides further guidance on filing a report.

6.3.6 Suspicions regarding previously obtained customer data

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

The gambling operator must make a case-by-case assessment of what information needs to be obtained. Based on the risk assessment, the gambling operator must decide whether to repeat the entire customer due diligence process 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 flagged and verified before the customer can use them for gambling. The purpose of this verification is to ensure that the customer is the rightful holder of the bank account linked to their gambling account and that the deposits come from legally obtained funds.

It is important that enhanced customer due diligence measures are implemented in a timely manner with regard to deposits. When a gambling operator detects suspicious activity, enhanced due diligence measures must be taken without delay. This means that these steps must be taken at the time of deposit, and not when the customer wishes to withdraw funds from their gambling account.

If a customer is unable to verify the origin of a deposit or refuses to provide information about the source of the funds, it **may** be appropriate to report the matter to the Financial Intelligence Unit. Chapter 7 of these guidelines provides more information about the Financial Intelligence Unit and filing reports.

6.4 Customer due diligence related to compliance with sanctions regulations and asset-freezing orders

As part of the customer due diligence measures prescribed in chapter 3 of the Anti-Money Laundering Act, an obliged entity must have effective policies, procedures and internal controls in place to ensure that it complies with the obligations imposed on it:

1) The decrees issued on the basis of Article 215 of the Treaty on the Functioning of the European Union, and the government decrees referred to in section 1 and section 2a, subsection 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 regulations); and
2) Decisions issued on the basis of section 2b of the Act referred to in 1) above and on the basis of the Act on the Freezing of Funds with a View to Combating Terrorism (325/2013) (asset-freezing orders).

According to the government proposal for the amendment of the Anti-Money Laundering Act (HE 323/2022 vp), ‘effective policies, procedures and internal controls’ refers to measures that, when implemented, enable obliged entities to detect and prevent activities that violate sanctions regulations and freezing orders. These measures include identifying the customer, verifying their identity, collecting customer information, and continuously monitoring the customer relationship, as well as comparing the customer information with current sanctions regulations and asset-freezing orders and the freezing of assets specified therein. When establishing effective policies, procedures and internal controls, obliged entities could build them in proportion to the scope of their operations, their geographical reach, and the nature and scope of the products and services they offer, among other factors.

At present, obliged entities must take into account international sanctions based on the decrees issued on the basis of Article 215 of the Treaty on the Functioning of the European Union, and the government decrees referred to in section 1 and section 2a, subsection 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 regulations). In addition to the sanctions, the identified risks are, in practice, also equivalent to the risks associated with asset-freezing orders referred to in chapter 3, section 16 of the Anti-Money Laundering Act.

The sanctions administered by the US Office of Foreign Assets Control (OFAC) apply to US entities or those operating in the United States, but they do not, as such, apply to European companies or non-US companies operating within the EU. A gambling operator operating in Finland can, therefore, decide independently whether to comply with these sanctions. The supervisory authority recommends complying with OFAC sanctions.

An obliged gambling operator subject to the Anti-Money Laundering Act must take into account the sanctions set forth in chapter 3, section 16 of the Act as a whole, even though, in practice, restrictions applying to natural persons who are customers of a gambling company will almost always involve various financial sanctions rather than, for example, restrictions on diplomatic relations or similar measures. When complying with sanctions regulations, obliged entities must use up-to-date sanctions lists, such as the European Commission’s consolidated list of persons, groups and entities subject to EU financial sanctions.

Only natural persons may be customers of a gambling company. A gambling company may offer online gambling only to individuals who have a Finnish personal identification number and are permanently resident in Finland. This can be considered to reduce the sanctions risk in Finnish gambling, so sanctions risks in the gambling industry are not currently deemed very likely. At physical locations, games may also be offered to individuals who do not have a permanent residence in Finland. The gambling operator must take this into account in its operations and risk assessments if it offers games at physical locations.

The consequences could be significant if a risk materialises, as this could lead to both money laundering and the financing of terrorism. The most significant risks identified in relation to sanctions and asset-freezing decisions in the gambling sector are personnel, system and customer risks.

The reform of the Anti-Money Laundering Act regarding customer due diligence related to sanctions regulations is relatively recent, so operational shortcomings related to personnel competence and the systems required for operations are possible. The personnel responsible for monitoring the operations must be trained to understand the principles of international sanctions and know how to respond in the event of a potential match on the sanctions list. This requires the obliged entity to have effective internal processes in place so that the legal requirement for effective policies, procedures and

internal controls can be deemed to have been met. In addition to enhancing personnel competence, it is essential to take into account the internal division of responsibilities within the obliged entity with regard to the arrangement of sanctions monitoring.

It is not justified to arrange sanctions monitoring in such a way that it is the sole responsibility of a single person if the scale of the obliged entity's business is significant in terms of the number of customers and revenue.

Systemic risks can be seen as another significant risk in the regulatory oversight of gambling operations. Effective sanctions monitoring requires robust and up-to-date systems that are capable of processing data from sanctions lists and the obliged entity's customer systems efficiently and reliably. To ensure that the systems function reliably in this regard, the systems should be regularly improved and tested. The systems should enable effective anti-money laundering monitoring when a new customer registers in the obliged entity's system. Similarly, monitoring should be organised in such a way that ongoing monitoring of customers can be carried out in a manner that allows for the identification of any customers on sanctions lists as close to real time as possible.

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

6.5 Statement of the source of funds

A statement on the source of funds is a key component of customer due diligence. When a new customer registers, the gambling operator must verify the source of the funds the player uses for gambling. Possible sources of funds include wages, benefits, savings and gambling winnings, among others. In addition, a statement on the source of funds must be obtained during the customer relationship if suspicions arise or a discrepancy is identified, for example.

Gambling operators must be vigilant regarding the statement on the origin of funds. The gambling operator must ensure that the information 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 source of the funds. **Simply crediting previous winnings back to a gambling account does not automatically mean that the funds are legitimate**.

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

Examples of situations in which the statement on the source of funds may not be sufficient or reliable:

- When registering, a customer indicates in the due diligence questionnaire that they are unemployed, but nevertheless reports the source of their funds as “earned income”
- When registering, a customer reports an income of, for example, €2,000 per month, but says that they gamble or actually gambles with significant sums
- A customer makes large one-off bets that are incompatible with their income level
- A customer states that the source of their funds is “gambling winnings”, but the gambling operator is unable to verify this

These examples are provided for guidance only and should not be considered 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.

Statements on the origin of funds are part of a gambling operator’s risk-based operations. The greater the risk involved (such as large, high-stakes bets or discrepancies in the information provided), the more thorough the measures required of the gambling operator. These measures may include updating customer due diligence procedures, contacting customers directly, and obtaining more detailed information.

6.6 Insufficient information provided by the customer

If a gambling operator is unable to carry out the customer due diligence measures prescribed in chapter 3 of the Anti-Money Laundering Act, it must not establish a customer relationship, conduct a transaction, or maintain a business relationship. A gambling operator may not, therefore, register a customer 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 business operations and prevent the customer from gambling until sufficient information has been obtained. If necessary, the gambling operator must report suspicious transactions to the Financial Intelligence Unit and terminate the customer’s account.

A gambling operator must not register a customer whose account it has previously terminated due to insufficient documentation. In such a situation, a customer may only re-register 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 Financial Intelligence Unit is part of the National Bureau of Investigation’s national intelligence operations. The mission of the Financial Intelligence Unit is to prevent, expose, detect and launch investigations into crimes and terrorist financing. The unit’s operations are controlled by the Act on the Financial Intelligence Unit.

The Financial Intelligence Unit's tasks include:

- Preventing, detecting and examining money laundering and terrorist financing, and launching investigations into such cases
- Receiving reports of suspicious transactions and terrorist financing, and providing feedback to obliged entities
- Cooperating with obliged entities and authorities
- Conducting operational and strategic analysis

The unit receives reports of suspicious transactions from obliged entities, processes and analyses relevant information, and provides it to other Finnish authorities. They are also involved in close international co-operation. The Financial Intelligence Unit has the right to receive, process and disclose information.

7.2 Report of a suspicious transaction

Under chapter 4 of the Anti-Money Laundering Act, a gambling operator must review and report suspicious transactions. A report can be filed even without evidence that money laundering or terrorist financing has actually taken place. If suspicions persist after further investigation, the matter must be reported to the Financial Intelligence Unit without delay.

A suspicious transaction refers to gambling activity that deviates from a customer's usual behaviour or is atypical of their gambling activities. Understanding the customer's normal actions, as discussed earlier in this guide, is therefore extremely important. 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 have sufficient knowledge of the customer and their usual behaviour.

If a gambling operator or its agent detects unusual gambling activity, it must investigate the reason. If, even after receiving an explanation, the gambling activity still appears suspicious, or if no explanation is provided at all, the matter must be reported to the FIU without delay. If an agent of a gambling operator notices a suspicious transaction, the agent should notify the gambling operator, which should report the matter to the FIU.

The FIU reporting channel is the goAML reporting system.

A gambling operator must register with the reporting system before submitting a report. Gambling operators must also comply with the regulation issued by the FIU regarding the format of suspicious transaction reports and the layout of their content. **This regulation applies to all obliged entities**. Gambling operators must familiarise themselves with the contents of the regulation.

Using the correct technical format of the reports and the layout of their content is essential for the FIU to carry out its statutory duties. For this reason, obliged entities are required to submit reports of suspicious transactions to the FIU 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 comply with the requirements may result in the FIU being required to report the non-compliance to the competent supervisory authority.

Submitting a notification to the FIU 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 intensifying the monitoring of the customer relationship. The gambling operator must, therefore, obtain sufficient information about the customer and must 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.

Operators should always decline suspicious purchases of gambling products or suspicious withdrawals of winnings. A report of a suspicious transaction must also be filed if a fact later comes to light that makes the gambling activity appear suspicious. A report of a suspicious transaction must therefore be filed regardless of whether the bet was accepted, suspended or declined.

Operators should have a low threshold for filing reports. A report to the FIU is not a crime report, and it is not the responsibility of the gambling operator or its agent to assess whether there is sufficient evidence for the incident.

The Anti-Money Laundering Act also contains provisions regarding the non-disclosure obligation. A gambling operator must not reveal to a customer or third party that it has filed or intends to file a report with FIU.

The FIU publishes an annual report in which it reviews reports of suspicious transactions received from various business sectors during the year. The number of suspicious reports submitted to the FIU has increased over the years across all sectors. The supervisory authority recommends that gambling operators monitor and review the FIU's annual reports.

7.3 Indicators of suspicious transactions in the gambling industry

The Financial Intelligence Unit has compiled a list of money laundering indicators that obliged entities should monitor. The purpose of this list is to assist obliged entities in identifying money laundering and suspicious transactions and in filing reports regarding such transactions.

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

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

The list of indicators is not exhaustive. In addition, a customer acting in one of the ways on the list does not necessarily indicate money laundering or other criminal activity. The purpose of this list is to identify the most common indicators for obliged entities in the industry from the FIU’s perspective. These indicators are based on both national and international trends and observations in the field of money laundering.

8 Use of agents

Under the Anti-Money Laundering Act, a gambling operator may delegate the customer due diligence measures prescribed by law to a third party, provided certain conditions are met. However, a gambling operator must bear in mind that, under chapter 3, section 7 of the Anti-Money Laundering Act, the operator is responsible for all its obligations under the Act. This means that the gambling operator is always liable for its agent’s violations and/or failures to comply with the obligations under the Anti-Money Laundering Act.

At retail outlets selling the gambling operator’s games, the gambling operator must identify and address the risks associated with potential breaches of anti-money laundering obligations in the sale of gambling services. The gambling operator must

ensure that the personnel selling gambling products have sufficient experience and knowledge of money laundering risks. Particular attention should be paid to ensuring that new employees have sufficient knowledge of anti-money laundering measures and the ability to identify suspicious transactions.

When offering gambling services at physical premises, the gambling operator must comply with the mandatory identification requirement set forth in section 28 of the Gambling Act. Customers must always be identified before they can gamble. In addition, customer due diligence measures must be carried out in the situations required by the Anti-Money Laundering Act (see chapter 6 of these guidelines). In addition, the individuals who sell gambling products must identify suspicious transactions and report them.

Gambling operators can reduce the risk of non-compliance with anti-money laundering obligations while also enhancing their employees' skills and knowledge by providing regular ongoing training and up-to-date information, including on money laundering indicators. Agents and other employees in positions of responsibility must be trained to identify and detect suspicious transactions, interconnected transactions, and instances where thresholds are exceeded. Only individuals who have received appropriate training on anti-money laundering laws and risk assessments should be involved in selling gambling products. The gambling operator must ensure that personnel who sell gambling services understand the importance of reporting suspicious transactions in order to prevent money laundering and the financing of terrorism.

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 related to money laundering and terrorist financing. An outsourcing agreement must be drawn up for the outsourcing. The gambling operator must ensure that the entity to which tasks are outsourced is familiar with the provisions of the Anti-Money Laundering Act and is capable of complying with anti-money laundering measures. The gambling operator must be aware that it is not exempt from its responsibilities under the Anti-Money Laundering Regulation, even if it outsources certain functions.

The adoption of the Anti-Money Laundering Regulation will begin in July 2027. The supervisory authority will issue more detailed guidance on outsourcing at a later date.

9 Training

Gambling operators have a legal obligation to train their personnel on the provisions of the Anti-Money Laundering Act. The purpose of training is to ensure that employees understand the importance of preventing money laundering, recognise the risks, and know how to comply with regulations. Training is part of the operator's overall obligation to prevent money laundering and maintain a trustworthy business environment for gambling.

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. Training must be up-to-date and comprehensive, and its content must be updated as the legislation or operational risks change. The gambling operator must, therefore, ensure that its personnel have up-to-date and sufficient knowledge of the provisions and obligations under the Anti-Money Laundering Act.

Training must ensure that personnel have the necessary skills to follow the gambling operator’s procedures and guidelines. The content of the training must be tailored to the employee’s duties and responsibilities and in accordance with the licenceholder’s general risk assessment.

Regular training provided to the personnel of a gambling operator must cover at least the following areas:

- The key provisions of the Anti-Money Laundering Act
- The customer due diligence obligation
- Identifying suspicious transactions
- The practical implementation of the reporting requirement
- Policies for dealing with suspicious situations

The training requirement applies to all persons who:

- Participate in customer service or payment processing
- Oversee gambling operations
- Are responsible for activities related to combating money laundering (e.g., compliance or risk management tasks)
- Serve in the company's senior management and decide on practical measures
- New employees must also receive training as part of their orientation before they begin their duties.

The gambling operator must document:

- The course content
- The training days
- The participants
- Any training materials

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

After completing the training, employees should be able to:

- Identify situations that may be related to money laundering or terrorist financing.
- Understand their own duties and responsibilities under the Anti-Money Laundering Act.
- Act in a timely manner and in accordance with the guidelines, such as filing an internal report or stopping a transaction if necessary.

Training can be conducted internally or with the help of an external specialist. Online training is an acceptable form of training, provided that the quality of the content and the ability to track progress are ensured. The training may include practical examples, case studies, and tests to assess proficiency.

Gambling operators have no legal obligation to train their agents and retailers on the provisions and obligations of the Anti-Money Laundering Act. However, it is in the gambling operator's own interest to train its agents and retailers, as the operator is always liable for any breaches or violations of the Anti-Money Laundering Act committed by its agents and/or retailers. The supervisory authority may therefore impose supervisory measures or sanctions on a gambling operator due to a breach or violation of the Anti-Money Laundering Act by an agent or retailer acting on its behalf.

The supervisory authority recommends that gambling operators provide adequate and regular training on the key obligations under the Anti-Money Laundering Act to their agents and retailers.

10 Internal control and whistleblowing system

10.1 Internal control

The gambling operator should have internal controls to prevent money laundering and terrorist financing, ensure compliance with the Anti-Money Laundering Act and the regulations and provisions issued pursuant to it, ensure the proper handling of customer and business data, and protect employees who report suspicious transactions (see section 10.2 "Whistleblowing System").

The gambling operator must designate a person or unit responsible for internal control. The designated person or unit is responsible for overseeing and coordinating anti-money laundering measures, maintaining internal guidelines, and reporting to the management and authorities.

The role of internal control is to regularly assess the risks of money laundering and terrorist financing associated with business operations, determine measures based on those risks (such as due diligence procedures, ongoing monitoring, and enhanced monitoring) and document the risk assessments and the measures taken based on them.

Internal control must develop and maintain up-to-date internal guidelines covering

- Customer due diligence procedures (know-your-customer or KYC)
- Identification and assessment of unusual transactions
- The practical implementation of the reporting requirement
- Data processing, storage, and confidentiality
- Internal reporting channel and reporting procedure
- Information exchange within a group of businesses, if applicable

A gambling operator's internal control measures include the obligation to regularly train personnel on prevention-related obligations. Chapter 9 of these guidelines provides more information on the training requirement.

For example, a gambling operator must assess the effectiveness of its internal controls through internal audits or other evaluation methods, address any deficiencies, and update its internal guidelines as necessary. The results of the monitoring and the measures taken must be documented.

The gambling operator's senior management is responsible for ensuring that internal controls are properly arranged. The management must regularly monitor the effectiveness of internal controls and address any deficiencies.

10.2 Whistleblowing system

Under chapter 7, section 8 of the Anti-Money Laundering Act, a gambling operator must have procedures in place that allow its employees or agents to report, through an independent channel, suspected violations of the Anti-Money Laundering Act and the regulations and provisions issued pursuant to it within the gambling operator (known as a whistleblowing system). This means that employees and contractors should have the opportunity to report internally if a gambling operator violates anti-money laundering rules.

Gambling operators must ensure that whistleblower protection is secure and effective so that employees can report concerns without fear of reprisal. These measures are a key part of the overall effort to combat money laundering and terrorist financing. It must be possible to submit a report through a dedicated, independent and anonymous channel.

The purpose of whistleblower protection is to:

- Encourage employees to report suspicions in good faith without fear of reprisal
- Protect whistleblowers from discrimination, retaliation or disciplinary action
- Ensure that reports are handled confidentially and appropriately

A gambling operator must:

- Introduce an internal reporting channel that employees can use to submit reports anonymously or confidentially
- Appoint a body to receive and process reports impartially and without delay
- Ensure that the identity and details of the whistleblower are kept confidential
- Document and store reports as required by law
- Take the necessary measures if a report is found to be justified

11 More about the prevention of money laundering and terrorist financing

The National Police Board also recommends consulting the following sources, which are mentioned 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 the mechanisms to be put in place by Member States for the prevention of 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 and Counter-Terrorist Financing Authority and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, and (EU) No 1095/2010 (“AMLA Regulation”).

Government proposal to parliament supplementing the government proposal (HE 236/2021 vp) on amending sections 3 and 20b of the Act on the Prevention of Money Laundering and Terrorist Financing and 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 | Statutes of Finland | Finlex

Act on the Financial Intelligence Unit (445/2017)

Act amending section 1 of the Act on the Freezing of Funds with a View to Combating Terrorism | 1162/2013 | Statutes of Finland | Finlex

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the assessment of money laundering and terrorist financing risks affecting the internal market and relating to cross-border activities (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 regulator-specific risk assessment on the prevention of money laundering and terrorist financing (2024). Preventing 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 format of reports regarding suspicious transactions and the layout of the content.

Financial Intelligence Unit (2025). Annual report of the Financial Intelligence Unit 2024.

Ministry of Finance publications – 2021:17. National Risk Assessment of 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 of 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
Gambling Administration
Konepajankatu 2, P.O.Box 50, FI-11101 Riihimäki
Tel. +358 295 480 181, police.fi