Spel inspek tionen

Guidance for combating money laundering and terrorist financing

Version 2
February 2025

spelinspektionen.se

Contents

1 Introduction

The Swedish Gambling Authority has actively conducted anti-money laundering supervision in the Swedish gambling market since the previous guidance in 2021. In a number of cases, this supervision has resulted in interventions against licence holders who have failed to fulfil their obligations under the Act on Measures against Money Laundering and Terrorist Financing (2017:630) (the Anti-Money Laundering Act). The shortcomings have mainly been attributable to licence holders' efforts in respect of customer due diligence, which were deemed insufficient. Therefore, this fourth edition of the guidance includes some clarifications in these respects. Otherwise, the text has been edited in both linguistic and structural terms. This guidance replaces previous editions.

The guidance is primarily aimed at licence holders for commercial online gambling and online betting. However, the content is such that it is relevant for other licence holders as well.

The Swedish gambling market is constantly changing, and in recent years it has seen extensive technological development and strong economic growth. The licence categories of commercial online gambling and betting are the primary drivers of economic growth. The risk of the gambling sector being exploited for money laundering purposes is deemed to be high, mainly due to high bets, winnings and high turnover[1].

A central premise of the anti-money laundering regulations is to prevent businesses from being used for money laundering and terrorist financing. However, the ability to operate efficiently should not be affected more than necessary. Balancing these interests requires a risk-based approach from licence holders. The risk-based approach must permeate the licence holder's efforts to prevent money laundering and terrorist financing, which means that the measures against money laundering and terrorist financing must be proportionate to the risks in the licence holder's operations.[2]

1 See, for example, the National Risk Assessment of Money Laundering and Terrorist Financing in Sweden 2020/2021, p. 117.

2 See Section 4.

The guidance is not a precise manual for how individual licence holders should operate, but it does provide a general and summarised description of licence holders' obligations under the most key elements of the anti-money laundering regulations. It also describes potential approaches to risk-based work and provides examples of effective measures. Anyone using the guidance must always assess whether the guidance is applicable in the case in question. Licence holders must always take into account aspects such as the provisions of the Anti-Money Laundering Act and the Swedish Gambling Authority's regulations and general recommendations on measures to prevent money laundering and terrorist financing (SIFS 2019:2) (the Swedish Gambling Authority's anti-money laundering regulations).

A new regulatory framework to prevent money laundering and terrorist financing

Sweden, along with other EU countries, is facing upcoming regulatory changes in respect of money laundering. A new legislative package was adopted by Member States on 31 May 2024. The purpose of this is to achieve a more detailed and harmonised regulatory framework. The legislative package will – among other things – replace large parts of the Fourth Money Laundering Directive[3] with a regulation[4] that will be binding and directly applicable as law in Member States.

The parts of the Fourth Money Laundering Directive that are not transferred to the regulation will be replaced by a new Anti-Money Laundering Directive.[5] A new authority, the Anti-Money Laundering Authority (AMLA), will also be established at EU level. The regulation will enter into force on 10 July 2027, and AMLA is expected to start operating in 2025.

3 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

4 Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/201.

5 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.

2 Money laundering and terrorist financing

What is money laundering?

The Anti-Money Laundering Act aims to prevent the financial sector, the gambling sector and several other industries from being used for money laundering or terrorist financing. The provisions of the Anti-Money Laundering Act are largely based on EU directives (the Anti-Money Laundering Directives)[6], which in turn are based on the recommendations of the Financial Action Task Force (FATF).

The definition of money laundering is set out in Chapter 1(6) of the Anti-Money Laundering Act, which states that:

For the purposes of this Act, "money laundering" means actions involving money or other property originating from crime or criminal activity that

1. may conceal the property's connection to a crime or criminal activity,
2. may facilitate the acquisition of the property or its value,
3. may facilitate the evasion of legal penalties, or
4. involve someone acquiring, possessing, claiming a right to or using the property.

Money laundering schemes differ, and they can be simple or more complex in their design. Cash transactions are not the only aspect to consider. Money that is already in the financial system can also be subject to money laundering. Consumption of criminally obtained funds is included in the definition of money laundering under the Anti-Money Laundering Act. In the Swedish gambling market, the consumption of criminal proceeds is regarded as being the most common form of money laundering.[7] Gambling can form part of a criminal lifestyle, which means that the person can lose significant sums of money, while any winnings can indicate legal income.

What is terrorist financing?

Terrorist financing refers to the financial support of terrorism. Contributing money is not the only aspect to consider. Terrorist financing also involves collecting money, providing money and receiving money intended to be used for terrorism. Terrorism is often funded by money of legal origin, which can make it particularly difficult to detect.

6 The first Anti-Money Laundering Directive was adopted in 1991. The EU has since adopted four further directives in this respect.

7 See, for example, the National Risk Assessment of Money Laundering and Terrorist Financing in Sweden 2020/2021, p. 118.

3 General risk assessment

The Anti-Money Laundering Act requires licence holders to take risk-based measures to prevent their operations from being used for money laundering and terrorist financing. This means that licence holders' resources should primarily be used at points within their operations where the risks of money laundering and terrorist financing are greatest. Less extensive measures are needed in areas where risks are lower.

Licence holders are required to carry out what is known as general risk assessment, a risk assessment of their own activities, so that they can maintain a risk-based approach.[8]

This general risk assessment is fundamental to all other initiatives aimed at preventing money laundering and terrorist financing. It should form the basis for the operation's procedures and other measures aimed at preventing money laundering and terrorist financing. The scope of the risk assessment is reliant on the extent and nature of the operation.[9]

The risk assessment must be documented. It must describe how the licence holder's products and services could be exploited for money laundering or terrorist financing purposes, and assess the chances of this occurring. All factors that may have a bearing on the risks of money laundering and terrorist financing are to be taken into account in the risk assessment, but particular attention must be paid to the types of products and services offered, customers, distribution channels and geographical risk factors.[10]

It is important to ensure that the risk assessment is kept up-to-date, and so it must be reviewed and updated regularly. The risk assessment must also be relevant and realistic, which requires licence holders to understand actual threats and vulnerabilities. This assumes that the organisation has a knowledge of money laundering and terrorist financing in a Swedish context. The above is fundamental to the effective application of the risk-based approach and requires licence holders to constantly keep track of the latest reports on money laundering and terrorist financing.

The situational analysis presented by the National Intelligence Centre[11] describes extensive organised crime in Sweden that is becoming increasingly complex.[12] Fraud is one of the most common crimes and a major source of income for criminals. Cash is a widely used payment method in the criminal economy, and there is a vast need to launder the cash proceeds of crime. Increasing numbers of young people being recruited into criminal networks is another growing problem.[13]

Criminals who use unlawful influence and infiltration of legitimate businesses to gain advantages are also described as a major societal problem.[14] This issue is linked to match

8 Chapter 2(1) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

9 Chapter 2(2) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

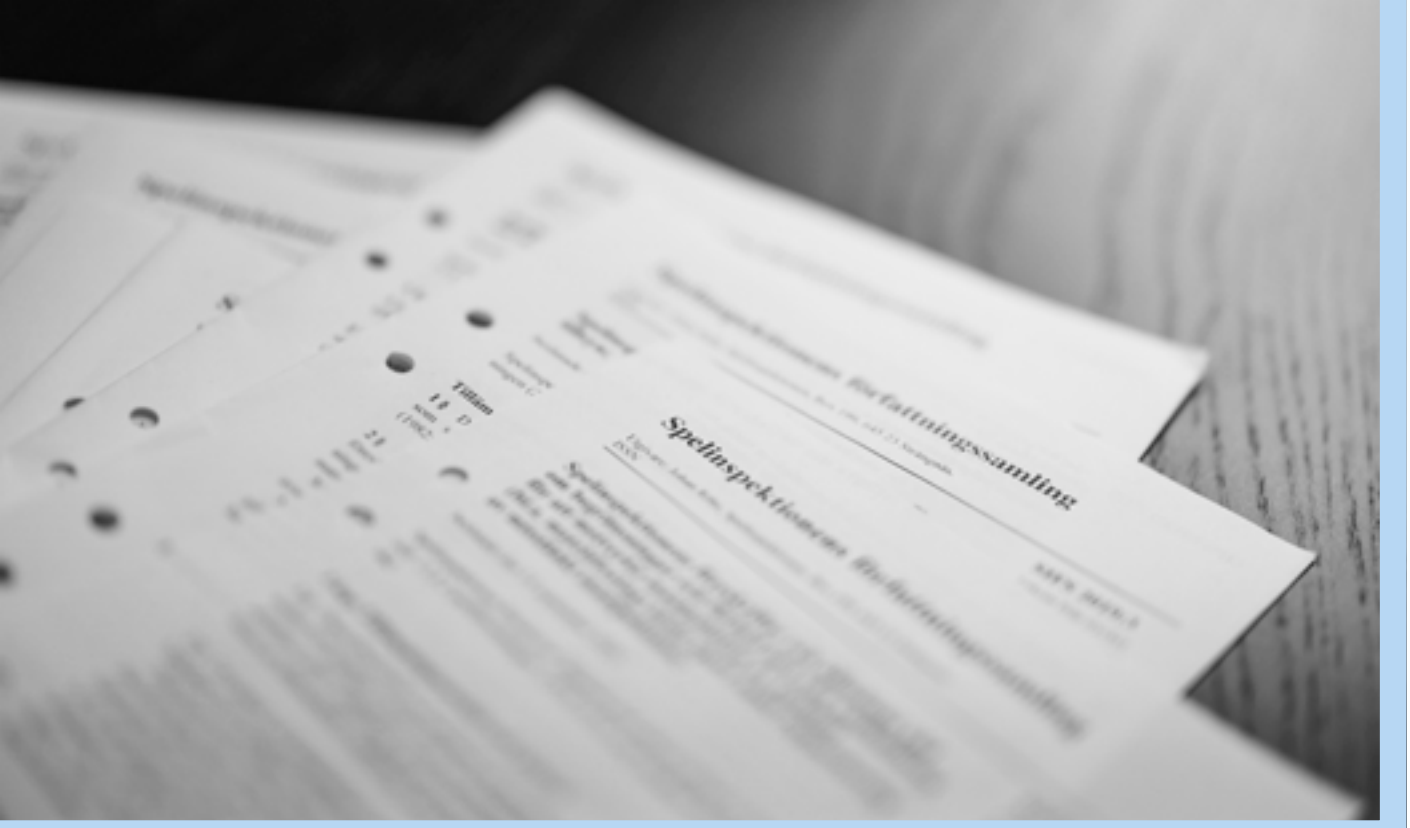
10 Chapter 2(1), second paragraph of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

11 The National Intelligence Centre is made up of thirteen authorities – including the Swedish Police Authority and the Swedish Economic Crime Authority – which form part of the joint government initiative against organised crime.

12 Swedish Police Authority – Myndighetsgemensam lägesbild, organiserad brottslighet 2023.

13 Swedish National Council for Crime Prevention report – Barn och unga i kriminella nätverk, 2023:13, p. 89.

14 Swedish Police Authority – Myndighetsgemensam lägesbild, organiserad brottslighet 2023, p.13.



fixing in sports and the gambling market. Match fixing can be used as part of a money laundering scheme where it is possible to make money while also laundering money. The National Operations Department is of the opinion that sports corruption in Sweden is becoming more widespread.[15] There is deemed to be a high risk of money laundering in the Swedish gambling market, and the consumption of the proceeds of crime is the most common form of money laundering in the sector.[16]

Licence holders have a responsibility to stay up to date on current risks and approaches to money laundering and terrorist financing through external monitoring, and to adjust their preventive measures to the prevailing circumstances in Sweden.[17]

Important relevant information and reporting in respect of money laundering and terrorist financing is provided by organisations such as the Coordinating Body for Anti-Money Laundering and Countering Financing of Terrorism (the Coordinating Body) and the Swedish Financial Intelligence Unit. The Coordinating Body works actively to identify risks and vulnerabilities in respect of money laundering and terrorist financing in Sweden and presents these regularly as part of a national risk assessment.

15 Swedish Police Authority, National Operations Department – Fenomenrapport om idrottskorruption, 2023, p. 3.

16 See, for example, the National Risk Assessment of Money Laundering and Terrorist Financing in Sweden 2020/2021, p. 118.

17 Chapter 2(1), second paragraph of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

4 Risk classification

Customer risk classification must be based on the general risk assessment of the operation and what the licence holder knows about the customer. Any new customer registering with the licence holder must be assigned a risk level.[18] The Anti-Money Laundering Act and the Swedish Gambling Authority's anti-money laundering regulations list circumstances that may indicate whether the risk is to be regarded as low or high.[19] This guidance also includes the 'normal' risk level in order to clarify what action the licence holder is expected to take for customer monitoring and surveillance.

It is important for the licence holder to monitor the customer's risk classification at regular intervals and adjust the risk level if so required. If the risk associated with a customer is deemed to be higher than when the business relationship was established, the licence holder must find out more information about the customer and intensify ongoing monitoring and surveillance if necessary. Monitoring and surveillance need not be as extensive or as frequent if the customer is deemed to be of lower risk.

The following indicators are recommendations provided by the Swedish Gambling Authority regarding what aspects should normally be taken into account when assessing the risk level, and when there is reason to adjust it. The deposit/gambling limits specified are based on Chapter 3(5) of the Anti-Money Laundering Act.

Indicators of low risk

The Swedish Gambling Authority is of the opinion that customers who make deposits totalling less than SEK 20,000 over a rolling[20] 12-month period may be regarded as low risk.

Indicators of normal risk

The Swedish Gambling Authority is of the opinion that customers who set deposit limits higher than SEK 20,000 and/or who gamble more than SEK 20,000 over a rolling 12-month period may be regarded as normal risk, unless there are indications that the customer should be classified as high risk.

Indicators of high risk

As stated in the Swedish Gambling Authority's anti-money laundering regulations, circumstances indicating a high risk may include unusual or irrational gambling patterns, unusually large transactions, and a reluctance to answer questions relating to customer due diligence or to submit documentation verifying the source of funds.[21] Note that if any of the above indicators is present, the licence holder must take appropriate action to manage the risk of being used for money laundering purposes, such as requesting information on the source of the funds.

18 Chapter 2(3) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

19 Chapter 2(4)– (5) of the Anti-Money Laundering and Terrorist Financing Act (2017:630) and Chapter 2(2)–(3) of the Swedish Gambling Authority's regulations and general recommendations on measures to prevent money laundering and terrorist financing (SIFS 2019:2).

20 'Rolling period' refers to a period that is always based on a specific time period going forward, instead of focusing on the calendar year.

21 Chapter 2(3) of the Swedish Gambling Authority's regulations and general recommendations on measures to prevent money laundering and terrorist financing (SIFS 2019:2).

5 Procedures

Licence holders must have risk-based procedures in place relating to measures designed to prevent money laundering and terrorist financing.[22] The purpose of these procedures is to mitigate the risks identified within the organisation. That is why it is important to maintain close links between the general risk assessment and the procedures.

Procedures must be in place regarding:

- Customer due diligence measures
- Monitoring and reporting
- Processing of personal data
- Suitability assessment of staff
- Compliance and internal control
- Procedures for model risk management, if such models are used

There are specific provisions on group-wide procedures for licence holders that form part of a group. The parent company in a group of companies must establish common procedures and guidance applicable to the group in its entirety.[23]

22 Chapter 2(8) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

23 Chapter 1(9)–(10) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

6 Training

The licence holder must ensure that relevant training and information are provided regularly to employees who perform duties that are essential to preventing the use of the organisation for money laundering or terrorist financing purposes.[24] This training must ensure that staff have sufficient knowledge to ensure compliance with the licence holder's procedures and guidance. The content of the training programme must be adapted according to the employee's duties and responsibilities and the licence holder's general risk assessment.

The timing of training and supplementary training must be adapted to what the licence holder concludes from its risk assessment, and to any changes in operations or duties.

More detailed requirements for the training programme are set out in the Swedish Gambling Authority's anti-money laundering regulations.[25]

24 Chapter 2(14) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

25 See Chapter 3(1) of the Swedish Gambling Authority's regulations and general recommendations (SIFS 2019:2).

7 Customer due diligence

Ensuring that there is sufficient knowledge of customers is a key element in preventing and obstructing misuse of the organisation for money laundering and terrorist financing. The customer due diligence process is primarily regulated in Chapter 3 of the Anti-Money Laundering Act and the Swedish Gambling Authority's anti-money laundering regulations. According to these regulations, certain information must always be collected and certain checks must always be performed. Without sufficient customer due diligence, the licence holder may not establish or maintain a commercial relationship or perform individual transactions.[26]

The initial check

The licence holder must identify the customer and verify the customer's identity through a reliable and independent source.[27] Besides the requirement for identification in the Anti-Money Laundering Act, the Gambling Act (2018:1138) stipulates that players must provide their name, address and personal identity number or equivalent when registering to gamble and that licence holders are obliged to verify the player's identity.[28]

In Sweden, e-identification such as BankID can be used to identify players under the Gambling Act. The Swedish Gambling Authority recommends that licence holders should always use e-identification for online identification. For customers who are initially classified as low risk, verifying e-identification and checking whether the customer is a politically exposed person (PEP) may, in many cases, suffice as a way of fulfilling simplified customer due diligence measures when customers register online.

Purpose and nature of the business relationship

The licence holder must also obtain information on the purpose and nature of the business relationship when the customer registers for gambling.[29] Obtaining information on the purpose and nature of the business relationship aims to provide the licence holder with grounds for assessing the risk that may be associated with the customer and how the customer is expected to behave within the framework of the business relationship. An assessment of this kind is necessary so that deviations from the anticipated behaviour can be detected.[30] The licence holder should find out how the customer is intending to use the gambling products or services, for instance.

In the case of gambling for money, recreational gambling and/or professional gambling can be presumed to be the purpose. The nature of the business relationship refers to the customer's anticipated gambling behaviour (gambling patterns), i.e. the frequency of transactions and the amounts deposited. As a rule, *entertainment* can be assumed the initial purpose of the customer relationship.[31] However, it is important to be mindful of the mandatory deposit limits that the customer has to set when gambling

26 Chapter 3(1) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).
27 Chapter 3(7) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).
28 Chapter 12(2) of the Gambling Act (2018:1138).
29 Chapter 3(12) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).
30 Government Bill 2016/17:173 p. 247.
31 Government Bill 2016/17:173 p. 248.

online.[32] If the deposit limits specified when the business relationship is initially established indicate that the customer will be gambling frequently and for large amounts of money, there is reason to examine more closely whether recreational gambling really is the purpose of the business relationship. This requires additional checks and verification of customer data.

In the light of the above, it is important for the licence holder to define the concept of *entertainment purposes*. Failing to do this will make it difficult for the licence holder to determine what actually constitutes unusual customer behaviour. According to Statistics Sweden, households allocated 9.2 per cent of their total expenditure to recreation, sport and culture in 2023.[33] This is an example of a gauge of *recreational consumption* and can provide an indication of when the customer should be assessed and their risk classification revised. The income situation in Sweden is another parameter that should be taken into account in the risk assessment. For instance, the median net income[34] in Sweden in 2023 was approximately SEK 320,000.[35]

To get to know customers better during the initial check, the Swedish Gambling Authority is of the opinion that licence holders should ask more questions when registering new customers. The licence holder's questions should focus on the origin of future deposits. Such information may lead to a better understanding of the purpose and nature of the business relationship and facilitate customer surveillance, monitoring and risk classification.

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

- Where will the funds that are to be used for gambling come from?
- What was your most recent annual income/where does your income come from?

Scope of customer due diligence measures

It is important for the licence holder to monitor the customer relationship continuously throughout the entire business relationship. Customer due diligence must always be kept up to date, and in-depth customer due diligence measures are required in order to understand and assess whether the customer's activities and transactions are legitimate and match the customer's risk profile.[36] The information collected about the customer should also be reliable and relevant. In Sweden, some relevant details, such as the registered address and income data, are public information and can be verified using external sources.

The customer's risk profile must be adjusted and additional measures must be implemented when a player deposits larger amounts, when total stakes are higher or when risks increase on account of other parameters. Enhanced measures, such as investigating the origin of the funds, must be implemented if the customer is deemed to present a high risk.[37] Enhanced customer due diligence measures must also be implemented in instances in which unusual activity or suspicious transactions and activities are observed

32 See Chapter 14(7) of the Gambling Act (2018:1138).

33 Statistics Sweden, Hushållens konsumtionsutgifter efter ändamål. Gambling for money is included in the consumption category 09 Recreation, Sport and Culture.

34 Net income is the sum of all of a person's taxable and tax-free income minus tax and other negative transfers (such as repaid student loans).

35 Statistics Sweden, Nettoinkomst för boende i Sverige hela året efter region, kön och ålder. Nettoinkomst, medianinkomst för boende i Sverige hela året, tkr efter region, kön, ålder och år [Net income, median income for residents in Sweden throughout the year, SEK thousands by region, sex, age and year] PxWeb.

36 Government Bill 2016/17:173 p. 249.

37 Chapter 3(16) of the Gambling Act (2018:1138).

within the context of the licence holder's monitoring of ongoing business relationships.[38] Thus, the customer does not necessarily have to have been categorised as high risk for enhanced measures to be applied.

The extent of the measures required is dependent on the complexity of the product or service and the risks that may be associated with the product/service or the unique business relationship.[39]

Large, unusual and/or irrational deposits should be stopped and verified before the customer has the opportunity to use the deposited funds. In this context, verification aims to ensure that the customer is the rightful owner of the bank account linked to the gambling account and that the deposits originate from funds acquired legally. In previous supervisory cases relating to money laundering, the Swedish Gambling Authority has noted that enhanced customer due diligence measures are often implemented too late in relation to when deposits are made. Enhanced customer due diligence measures must be implemented promptly and as soon as possible when licence holders detect suspicious transactions.[40] In other words, it is important for these measures to be implemented immediately; when the deposit is made, for example, and not just when the player requests a withdrawal from their gambling account.

There may be grounds to report the customer to the Financial Intelligence Unit if the customer is unable to verify the deposit or is reluctant to disclose the origin of the money.

In a risk-based approach, the measures must be proportionate to the risks. For instance, it may be appropriate to obtain information on annual income in the case of normal risk, whereas additional verification and contact with the customer may be required to determine the source of the customer's funds in the case of high risk.

Closed loop as a risk mitigation measure

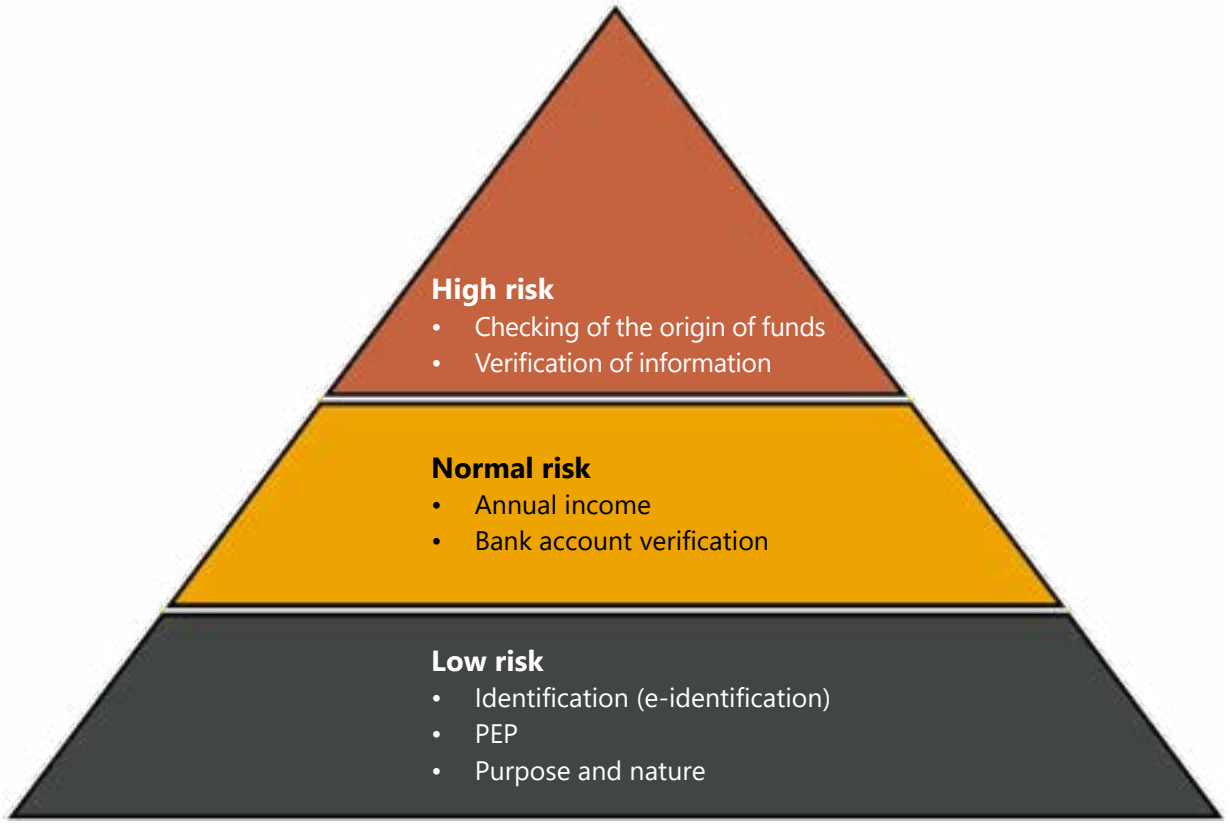
Licence holders that provide multiple deposit and withdrawal options should be particularly vigilant with regard to the fact that deposits and withdrawals may be made to different accounts. One way of mitigating certain risks relating to money laundering and terrorist financing may be to apply what are known as closed loop transactions, which means that the customer can only withdraw funds to the account from which the deposit was made. This can be achieved by allowing the customer to use only one account for all transactions.

It should be added that the existence of closed loop transactions does not ensure that deposits to a gambling account originate from funds acquired legally. The Swedish Gambling Authority's anti-money laundering supervision has demonstrated that it is common for licence holders to use net deposits/previous gambling winnings as a basis and assume, without obtaining further information, that the funds originate from previous

38 Chapter 4(1)–(2) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

39 Chapter 2(1) and Chapter 3(14) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

40 See the ruling of the Administrative Court of Linköping in case no. 7081–21.



The diagram summarises how customer due diligence measures at different risk levels may vary, as described below.

withdrawals from the gambling account. To verify the origin of the funds, it is usually necessary to check bank statements in order to confirm that the funds are, for example, winnings that were paid out by the licence holder and redeposited to the gambling account.

For customers to be categorised as **low risk**, measures that involve identifying the customer and checking for PEP status must have been implemented as a minimum. Regardless of the level of risk, the licence holder must obtain information on the purpose and nature of the business relationship. This information must also be evaluated regularly.

In addition to the above measures, customer due diligence measures for **normal risk** should include the collection of data on annual income. If necessary, verification of bank accounts may also be required.

All of the measures indicated above must be implemented if the customer is deemed to be **high risk**. Additional information about the customer should be obtained in the form of information on the origin of the funds (SOW/SOF).[41] The origin of funds refers to detailed information about the customer's financial situation and the source of the funds deposited in the gambling account. Verification of information must ensure that the details are correct and consistent with what the customer has stated.

41 Chapter 4(2) of the Swedish Gambling Authority's regulations and general recommendations on measures to prevent money laundering and terrorist financing (SIFS 2019:2).

8 Retention of documents and information

Rules on documentation and how personal data is to be stored are set out in Chapter 5 of the Anti-Money Laundering Act. This states, among other things, that the licence holder is obliged to retain customer due diligence documents and data, data on transactions implemented within a business relationship and individual transactions covered by the customer due diligence requirement.

Licence holders must retain documents and data relating to measures undertaken for customer due diligence purposes for five years.[42] Such documents and data must be dated, in accordance with the Swedish Gambling Authority's anti-money laundering regulations.[43]

42 Chapter 5(3) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

43 Chapter 6(1) of the Swedish Gambling Authority's regulations and general recommendations (SIFS 2019:2).

9 Model risk management

There must be procedures in place for model risk management if the licence holder uses models for risk assessment, risk classification, surveillance or similar. These procedures must aim to evaluate and ensure the quality of the models used by the licence holder.[44] The term 'model' refers to procedures that aim to automate or standardise the assessments and other procedures implemented by operators in order to ensure compliance with the various requirements of the Anti-Money Laundering Act.[45] Examples include automated monitoring systems that are programmed to warn of or flag transactions that are considered by licence holders to be associated with high risk or otherwise considered to be unusual.

The scope and content of the procedures and guidance must be determined on the basis of the size and nature of the licence holder and the risk of money laundering and terrorist financing as identified in the general risk assessment.[46]

44 Chapter 6(1) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

45 Government Bill 2016/17:173 p. 547.

46 Chapter 2(2) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

10 Monitoring

Within the framework of the customer due diligence requirements of the Anti-Money Laundering Act, licence holders must continuously monitor the business relationships with their customers.[47] Ongoing monitoring of the business relationship serves two purposes. One purpose is to ensure that what is known about the customer is up-to-date, correct and sufficient to justify the risk that may be associated with the customer. The second purpose is to detect unusual transactions and activities in order to prevent the customer from attempting to launder money or finance terrorism.[48]

Licence holders must monitor and review transactions and activities in accordance with Chapter 4(1) of the Anti-Money Laundering Act in order to detect deviations from expected behaviour.

This involves checking and documenting that the transactions carried out are consistent with company's knowledge of the customer, its business and risk profile and, if necessary, the source of the customer's funds. Enhanced customer due diligence measures must be implemented if the licence holder becomes aware of deviations from the expected behaviour.[49]

The extent and frequency of surveillance and review are dependent on the risks associated with the business relationship in question.

47 Chapter 3(13) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

48 Government Bill 2016/17:173 p. 249.

49 Chapter 4(2) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

11 Reporting to the Financial Intelligence Unit

The mission of the Financial Intelligence Unit is to act as the Financial Intelligence Unit for Sweden and to form part of national intelligence operations within the Swedish Police Authority. The Financial Intelligence Unit handles information on predicate offences for money laundering, or when money laundering is suspected to be involved in an attempt to conceal the proceeds of crime. The Financial Intelligence Unit also handles information relating to terrorist financing.

Under Chapter 4 of the Anti-Money Laundering Act, licence holders are obliged to review and report suspicious transactions. To file a report, there does not need to be any evidence that money laundering or terrorist financing has actually taken place. If the suspicion persists after the matter has been reviewed, a report must be filed with the Financial Intelligence Unit without delay.

No further measures in the form of enhanced customer due diligence measures need to be implemented if the licence holder has concluded that there are reasonable grounds to suspect money laundering or terrorist financing as described above.[50] Reporting a matter to the Financial Intelligence Unit does not automatically require the termination of a business relationship. However, it should be added that the licence holder is always obliged to terminate a business relationship if the licence holder lacks sufficient knowledge of the customer to be able to manage the risk of money laundering or terrorist financing.[51] Given this fact, filing a report with the Financial Intelligence Unit should lead the licence holder to reassess the risk presented by the customer and enhance its surveillance of the business relationship.

50 Chapter 4(2), second paragraph of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

51 Chapter 3(1) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

The Anti-Money Laundering Act contains rules on confidentiality, which means that disclosure without authorisation to the customer or any third party that a report has been or will be filed with the Financial Intelligence Unit is not permitted.[52]

The number of suspicious transactions reported to the Financial Intelligence Unit has increased across all industries over the years. The gambling industry accounted for 9 per cent of all reports filed in 2023. To ensure that information is handled as effectively as possible, the quality of reports is of great importance to the Financial Intelligence Unit. That is why it is important for the report to include all the circumstances that support the suspicion, and for it to adhere to the data structure of the goAML reporting system. In many cases, the Financial Intelligence Unit rejects a number of reports because basic information is missing, or because the person filing the report failed to describe with sufficient clarity why the transaction or behaviour was considered suspicious.[53]

Find out more about reporting to the Financial Intelligence Unit and report cases here:

https://polisen.se/om-polisen/polisens-arbete/finanspolisen/

https://fipogoaml.polisen.se/Home

52 Chapter 4(9) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

53 Finanspolisens årsrapport 2023 (the Swedish Financial Intelligence Unit's annual report for 2023), p. 9.

12 Internal control and whistleblowing

Size and nature of the organisation

Chapter 7 of the Swedish Gambling Authority's anti-money laundering regulations contain more detailed provisions on cases in which the licence holder is obliged to appoint a specially designated officer and a central function officer and establish an independent review function. This chapter states that licence holders are obliged to establish these functions if their operations had stakes before paid-out winnings of at least SEK 50 million in the previous financial year. If such information is unavailable, whether the licence holder has stated in its licence application that the estimated stakes before paid-out winnings are at least SEK 50 million will be considered instead.

If so justified by the size and nature of the organisation, the licence holder must appoint:

- A member of the management team, managing director or equivalent officer to stand responsible for ensuring that the licence holder implements the measures required under the Anti-Money Laundering Act.
- A central function officer who is responsible for continuously verifying that guidance, controls and procedures are in place to effectively manage the organisation's money laundering and terrorist financing risks and to ensure that reports are filed with the Financial Intelligence Unit.
- An independent audit function that is responsible for verifying that the licence holder is operating in compliance with the Anti-Money Laundering Act.

Whistleblowing system

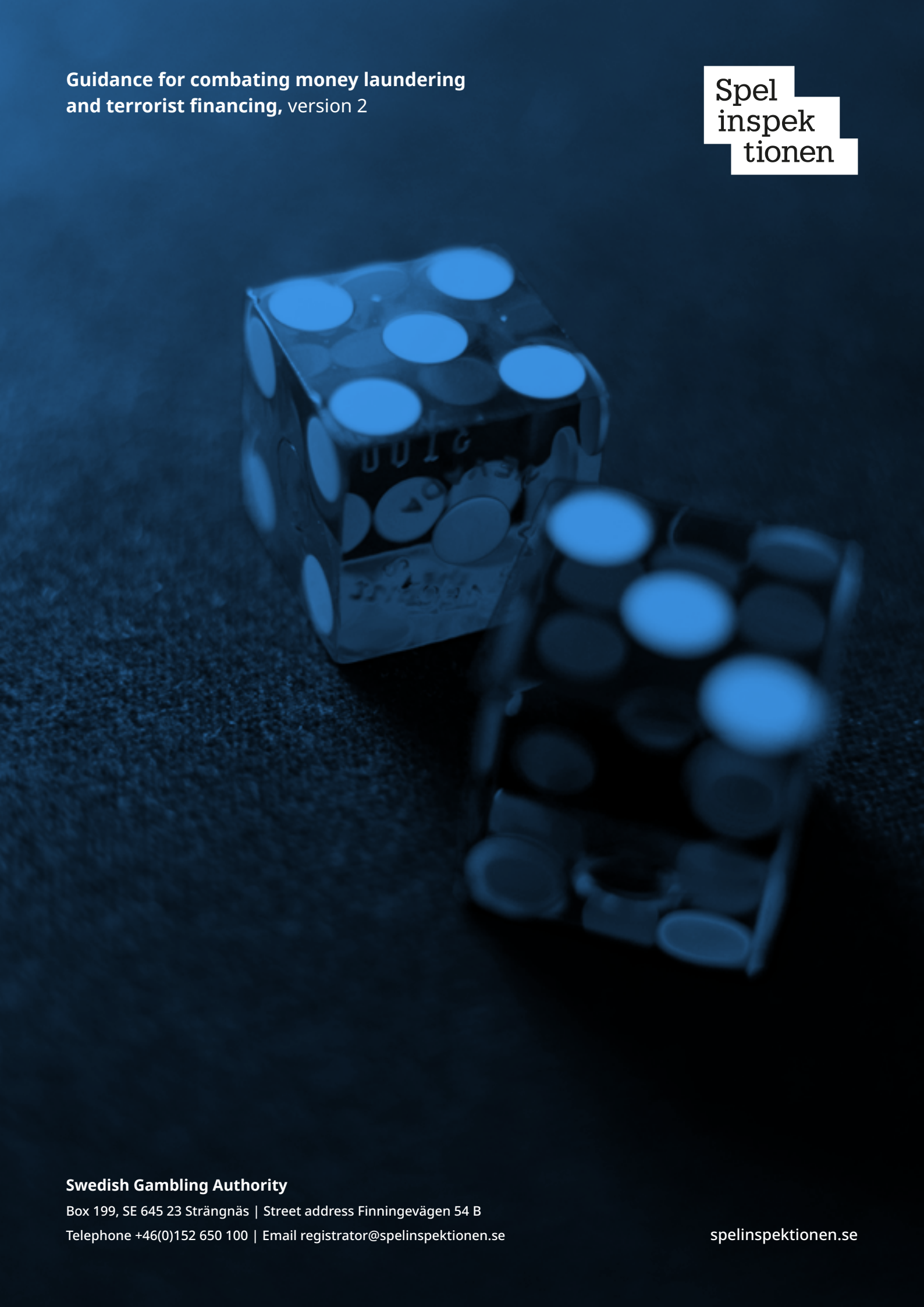
Under the Anti-Money Laundering Act, the licence holder must ensure that whistleblowing systems are in place, which means that there must be an opportunity for employees and contractors to file reports internally if the licence holder breaches the money laundering regulations.[54] These reports must be filed via a dedicated, independent and anonymous channel.[55]

54 Chapter 6(4) of the Anti-Money Laundering and Terrorist Financing Act (2017:630).

55 Chapter 7(12) of the Swedish Gambling Authority's regulations and general recommendations on measures to prevent money laundering and terrorist financing (SIFS 2019:2).

Guidance for combating money laundering and terrorist financing, version 2

Spel inspek tionen



Swedish Gambling Authority
Box 199, SE 645 23 Strängnäs | Street address Finningevägen 54 B
Telephone +46(0)152 650 100 | Email registrator@spelinspektionen.se

spelinspektionen.se