10. Vulnerability of the gambling sector

10.1. General description of the sector

Table 55. Description of the gambling sector.

Market participants	Number of market participants as of 31.12.2019	Number of obliged entities	Existence of a professional association or umbrella organization
Gambling operators	20	100%	Estonian Gaming Operator Association

Number of market participants

In Estonia, with a permit, it is possible to organize games of chance, toto, lotteries, games of skill, and commercial lotteries as land-based or as remote gambling. As of December 2020, 21 companies in Estonia have various activity licenses for the organization of gambling in Estonia[1]. One company may have an activity license to organize several different types of gambling. The lottery can be organized in Estonia only by a public limited company, all shares of whose are held by the Estonian state - i.e., it is a state monopoly. The number of companies organizing gambling in Estonia by the type of gambling is as follows:

- Land-based games of chance - 3;
- games of chance on ships - 1;
- remote gambling games of chance - 16;
- land-based toto - 2;
- remote gambling toto - 14;
- lottery - 1.

Table 56. Survey data from the gambling sector.

Sector	Number of market participants	Sample size	Sample size/ number of responses required	Number of invitations sent	Number of responses received
Gambling operators	20	all	19	19	19

During the survey period of the NRA, there were 20 licensed market participants, four of whom were licensed to operate gaming locations, with one gaming operator managing gaming locations only on ships. Of this sample, 19 market participants responded to the survey, including all four land-based or onboard gambling companies; therefore, the response to the survey provides a meaningful overview of the market players in the gambling sector as a whole and the practices they actually practice.

Number of toto and gambling locations

In Estonia, a separate operating permit is issued for each land-based toto and gambling location and one joint operating permit for toto offered on the Internet and remote gaming. As of December 2020, the number of gaming locations for operating gaming and toto on land and on ships in Estonia is as follows:

- land-based gaming locations for a game of chance – 55,
- gaming locations for a game of chance on ships – 6,
- land-based gaming locations for toto - 25.

[1]Information on operators and permits from the Register of Economic Activities (https://mtr.mkm.ee/).

The professional association or umbrella organization for gambling providers in Estonia is the Estonian Gaming Operator Association (hereinafter EGOA), which includes all land-based gambling operators and many remote gambling operators. As of December 2020, EGOA has 11 members.[2]

Specificity of the sector

The Gambling Act imposes strict requirements on gambling operators, which help to ensure the trustworthiness of companies and their employees in the sector, oblige them to identify customers and make the movement of money more transparent. Due to the fact that the gambling sector is highly regulated, the fulfillment of the gambling sector requirements makes it, in comparison with the other sectors, significantly easier for each market participant to comply with the requirements arising from the Money Laundering and Terrorist Financing Prevention Act (MLTFPA).

Legal framework

In 2000, the scope of the MLTFPA in Estonia was extended to gambling operators. As regards the prevention of money laundering and terrorist financing, the sector is mainly regulated by the MLTFPA, according to which[3] all the market participant of the gambling sector in Estonia, except for the operators of a commercial lottery[4], are obliged entities.

The Gambling Act (GA) regulates in detail the aspects of organizing gambling and the requirements for obtaining an activity license for organizing gambling and operating permit for organizing gambling. A trustworthy legal person who meets the requirements of GA and who has the activity license for organizing gambling, and operating permit for organizing gambling has the right to organize a game of chance, toto, or a game of skill. The right to organize a lottery is granted to a trustworthy person that meets the requirements of GA and who has received an operating permit for organizing lotteries.[5]

Money laundering and terrorist financing offenses are criminalized in the Penal Code, which also criminalizes the provision of premises for the purposes of illegal gambling[6] as a possible predicate offense related to the activities of the sector. Money laundering misdemeanors are regulated by the MLTFPA. In all the above-mentioned acts, it is possible to hold liable both the gambling operators as the legal person and the natural person who committed the offense.[7]

The regulatory authority of the sector is the Tax and Customs Board (TCB), which also supervises the sector. The FIU has supervisory competence over the requirements of MLTFPA, and, if necessary, it is possible to exercise supervision jointly.

Requirements and background checks for gambling operators and their related persons and employees

As gambling companies need to be trustworthy, a thorough background check is carried out on those involved. For example, a shareholder with a qualifying holding, beneficial owner, or a member of the management body of a gambling operator may not be a person who has offense criminal record or a person who has been a member of the management body of a legal person that has organized gambling without an activity license or operating permit or whose activity license has been revoked, or if it appears from the court judgment in the

[2] http://www.ehkl.ee/et (28.12.2020).
[3] § 2 (1) (3) of the MLTFPA provides that the law applies to gambling operators, except for operators of commercial lotteries;
[4] A commercial lottery is a classic or instant lottery organized under national law by a supplier of goods or services to promote the sale of goods or services or to advertise goods, services or their supplier. The right to participate in a commercial lottery is acquired together with the acquisition of goods or services. Requiring additional financial obligations from a participant in a commercial lottery is prohibited. Thus, at the legislative level, the approach chosen is a form of gambling organized by dealers, which in many countries is not regulated as gambling at all, so the money laundering risks of commercial lottery operators are thus essentially the risks of dealers, not the threats of gambling operators.
[5] § 9 (1) of the GA.
[6] § 268 of the Penal Code. Allowing illegal activities.
[7] Pursuant to subsection 14 (1) of the Penal Code, In the cases provided by law, a legal person shall be held responsible for an act which is committed in the interests of the legal person by its body, a member thereof or by a senior official or competent representative. Pursuant to subsection (2) of the same section, prosecution of a legal person does not preclude prosecution of the natural person who committed the offence.

bankruptcy proceedings that the person has caused the insolvency of the company due to a grave error in management.[8] Before acquiring a qualifying holding in a gambling operator or increasing such holding so that its proportion in the share capital of the gambling operator or all rights related thereto or votes represented by shares will exceed above 20, 30, or 50 percent, a person shall submit detailed information and documents to the TCB.[9] The TCB also makes a background inquiry to the FIU about the company and persons related to the company, asking for information that may call into question their trustworthiness and also prevent them from participating in the management of business activities.

The gambling operator must also ensure that the person punished for a criminal offense does not have the task of organizing gambling, making a decision on the right to participate in gambling, or carrying out supervision of gambling.[10] At least once a year, the TCB conducts a background check of the criminal record for all employees of gambling companies.

The obligation of gambling operators to identify players

According to the Gambling Act, all gambling operators must identify a player before they are allowed to play.[11] Land-based casinos identify a player upon entering the casino on the basis of an identification document. In the case of toto and the lottery, the person must be identified before accepting bets from the player. In the case of remote gambling, persons are identified using software solutions (mobile ID, ID card, bank link, requesting a copy of a document, and other means approved by the TCB). This makes it impossible to visit the gaming location or play remote gambling anonymously or using false information.

Requirements for a remote gambling operator on receiving and paying out payments

The remote gambling operator must ensure the acceptance of payments transferred to the account of the gambling operator for the making of bets only from the settlement account of the same player or from a player in the gaming location of the same gambling operator and the making of distributions only to the same settlement account, from which the player has transferred a payment to the account of the gambling operator for the making of bets in gambling.[12] Therefore, in the case of remote gambling (including online casinos), the movement of funds is transparent, and it is not possible to use bank accounts belonging to other persons or companies for depositing or withdrawing money.

Brief summary

All companies operating in the gambling sector are obliged entities within the meaning of the MLTFPA and are therefore subject to extensive requirements and supervision. The sector is not only subject to the broad obligations arising from the MLTFPA, but the entire gambling sector is regulated by a strict specific law (GA), as a result, only natural and legal persons with impeccable backgrounds can operate in the sector, whose activities are supervised and which makes the sector more transparent, also in terms of the prevention of money laundering and terrorist financing.

10.2. Description of threat typologies

In both casinos and remote gambling, it is theoretically possible to launder money using various schemes. The most common schemes are match-fixing, including deliberate losing, as well as the purchase of winnings, tokens, and tickets, as some of the possible ways to legitimize property derived from criminal activity. Theoretically, various casinos could be used for money laundering, where money is exchanged for tickets and later returned for cash without betting or betting small amounts. In the course of a transaction and service monitoring, a number of such attempts have been identified. As a countermeasure, market participants implement internal control mechanisms (both fully automatic and semi-automatic) and train their employees to recognize such schemes.

[8] § 9 (3) of the Gambling Act.
[9] § 11 (2) of the Gambling Act.
[10] § 33 (1) 3) of the Gambling Act.
[11] § 37 (8), § 53 (1) of the Gambling Act.
[12] § 53 (5) and (6) of the Gambling Act

Structuring, or 'smurfing,' involves splitting large amounts of cash into a number of smaller transactions to minimize suspicion and avoid reporting requirements. Refining involves the exchange of low denomination cash for a higher denomination currency. In response, more and more land-based gambling operators have moved to a loyalty card system, and internal controls are in place. Employees are trained to recognize and monitor situations where tokens or tickets are collected.

In the case of remote gambling operators, bets and payouts are made through credit and payment institutions, which are also obliged entities, but their limited knowledge may, in turn, make it more difficult to identify riskier customers and different schemes.

10.3. Threats

10.3.1. Threats of money laundering

High cash flow, number of transactions, and the share of cash

In the gambling sector, a large amount of money is moved; in casinos, a considerable part of it is moved in cash. The number and diversity of transactions make gambling an attractive way to launder money, encouraging so-called "playing through" the proceeds obtained via criminal means. The number of land-based casinos is on a downward trend; as of December 2020, there are four gambling companies operating on land or on ships. The largest market player in land-based gambling has moved to a loyalty card system. The operators use *tickets* and tokens instead of cash. Irrespective of whether the payment is made in cash or electronically (for example, by bank card), due diligence applies. The gambling operator shall apply due diligence measures at least in the event of a payout, a bet, or both if the amount given or received by the customer is at least EUR 2000 or the equivalent amount in another currency, regardless of whether the financial obligation is met in a single lump sum or in several linked payments over a period of up to one month.[13]

Insufficient number of initiated proceedings and cases

In the gambling sector, very few proceedings are initiated in connection with money laundering, and the knowledge that money is being laundered through gambling comes to light in practice in the framework of other cases. Gambling operators send many reports to the FIU, but most of them are amount-based, and few of them concern the suspicion of money laundering. Consequently, one potential threat may be that money laundering through the gambling sector is a crime that is difficult to detect and prove in practice.

The threat of creating illegal gaming locations

Attempts are often made to create remote gambling site without a license. The operators are mostly abroad, but in order to restrict these channels on Estonian soil, the TCB has had to block hundreds of such pages in recent years. Nevertheless, there is a threat that illegal playgrounds may go undetected.

Variability in the implementation of due diligence measures between market participants

There may be variations in the application of due diligence measures by gambling operators. This may be, in particular, the case for remote gambling operators. No significant shortcomings have been identified in practice, but no regular and comprehensive inspections have been carried out.

High-risk customers

In the case of gambling operators, the share of non-resident customers is higher than average. However, market participants also pay close attention to riskier customers when implementing due diligence measures[14], which reduces the threat arising from high-risk customers.

[13] § 19 (3) of the MLTFPA.
[14] According to the survey.

Use of virtual assets

The Gambling Act does not regulate transactions with virtual assets. At the moment, the Tax and Customs Board requires that the virtual asset wallet must belong to the player, but this measure may not be sufficient to prevent the threat of money laundering with virtual assets.

The anonymity of virtual assets allows them to be misused for criminal purposes. The inclusion of virtual and official currency exchange service providers and wallet service providers does not definitively solve the problem of anonymity in virtual asset transactions, because much of the virtual asset environment remains anonymous, as users can make transactions without such providers.[15]

Playing with unverified bank and credit cards

In land-based casinos, there is no obligation to verify the player's ownership of the bank and credit cards used for playing. Therefore, it is theoretically possible that someone else's bank card may be used for playing. In addition, there is a possibility that a bank card belonging to a company, for example, can also be used to gamble. It also provides an opportunity to launder the proceeds derived from criminal activity committed by legal persons and, in addition, to commit tax offenses.

10.3.2. Conclusion

Table 57. The threat level of money laundering in the gambling sector.

Sector	The threat level of money laundering at the sectoral level	
Gambling sector	1.95	**average/low**

The level of money laundering threat in the gambling sector is **average/low**, as a small number of gambling operators and a very high level of regulation have significantly mitigated several, money laundering risk factors. Market participants also have internal control mechanisms in place (both fully automatic and semi-automatic), and employees are trained to recognize such schemes. On the other hand, a large amount of money is moved through the gambling sector; in casinos, a considerable part of it is also in cash. The number and diversity of transactions make gambling an attractive mean to launder money, encouraging the so-called "playing through" of the proceeds obtained via criminal means. Therefore, it cannot be considered that the threat is non-existent or minimal.

10.3.3. Threats of terrorist financing

The threat of terrorist financing in the gambling sector is minimal. With regard to the prevention of terrorist financing, all gambling operators are subject to strict obligations analogous to the prevention of money laundering, including the obligation to apply due diligence, the obligation to provide information based on amount and suspicion, etc. – therefore the aspect of terrorist financing is mostly not considered or analyzed separately in the gambling sector. On the other hand, the use of schemes specific to terrorist financing in the context of the gambling sector would be largely inefficient or even impossible. Therefore, in practice,[16] an assessment of the threats of terrorist financing has not been found to be practical or appropriate for the gambling sector.

10.3.4. Conclusion

Table 58. The threat level of terrorist financing in the gambling sector.

Sector	Level of terrorism threat at the sectoral level	
Gambling sector	1.40	**low**

The threat of terrorist financing in the gambling sector is **low**.

[15] See FIU "Survey of Virtual asset Service Providers" 22.09.2020.
[16] E.g., SNRA 2019.

10.4. Vulnerabilities

10.4.1. Vulnerabilities of prevention of money laundering

10.4.1.1. Exposure to the threat

Threat related to large cash flows, the number of transactions, and share of cash:
The turnover of the gambling sector is high, and a significant part of transactions in casinos take place in cash. It is important to note that the popularity of remote gambling is on the rise, and for example, the bets in remote gambling have multiplied over the last few years.
Games of chance organized as remote gambling - bets (in euros):
2017: 955,678,475.42.
2018: 945,221,560.42.
2019: 1,641,248,282.27.
2020: 2,047,873,109.72.

On the other hand, during the same period, there has been a downward trend in the bets on gaming machines, which have traditionally operated in land-based casinos.
Gaming machines - bets (in euros):
2017: 621,559,100.17.
2018: 346,278,941.71.
2019: 571,309,607.63.
2020: 238,842,918.97.

The turnover of the gaming tables traditionally operated in land-based casinos has also been stable or slightly on the rise, but the data for 2020 that was not available at the time of writing might probably be lower than in previous years due to the global Covid-19 pandemic and related constraints.
Gaming tables - bets (in euros):
2017: 35,475,025.
2018: 35,823,516.
2019: 45,503,064.

The use of cash in the gambling sector is on a downward trend, as evidenced by the fact that market participants are increasingly favoring and moving to loyalty card systems; such an assumption can also be made in part from the FIU statistics - the amount-based notifications decrease and the number of threat-based notifications increases. Also, looking at the significant increase in the turnover of remote gambling operators and the changes in the turnover of gaming tables and machines, it can be concluded that the share of cash in the sector as a whole is decreasing. The number of land-based casinos is also on a downward trend: As of December 2020, there are four land or ship-based gambling companies.[17] There are no cash transactions with the remote gambling operators, as the payments made by the customer and the payments made to the customer are made through the accounts of credit or payment institutions, which means that there is no risk of cash transactions in organizing remote gambling.

The threat associated with a small number of proceedings and cases:
In 2019, gambling operators sent 250 reports to the FIU, which came from seven different reporters and accounted for 4.5% of all reports. The majority of reports (89%) came from one reporter, a total of 97% of reports came from two reporters. The majority of reports, 159 in total, were reports on cash transactions above the threshold or cash transactions unusual that were unusual (CTR). A total of 15 reports of suspicion of money laundering were submitted, of which six were unusual transaction reports (UTRs), five were suspicious transaction reports (STRs), and four were unusual activity reports (UARs). Gambling operators also sent 75

[17] Information on operators and permits is available from MTR at https://mtr.mkm.ee/. The information is also available on the website of the Tax and Customs Board https://www.emta.ee/et/eraklient/maa-mets-soiduk-kutus-hasartmang/seaduslike-hasartmangukhoitajate-nimekiri.

terrorist financing reports (TFR) and an international sanctions report (ISR). On the other hand, very few proceedings are initiated in the gambling sector in connection with money laundering, and in practice, the knowledge that money is being laundered through the gambling sector is revealed in relation to other cases. This may indicate that money laundering through the gambling sector is a difficult crime to detect and prove, which is why the number of notifications is low (except for amount-based notifications).

Threat associated with the creation of illegal gambling sites:
In 2019, the TCB blocked 83 unlicensed remote gambling sites, and by October 2020, another 52 sites had been blocked. Over the years, the Tax and Customs Board has blocked a total of 1,631 pages. As these are usually not pages that would have a linkage with Estonia (for example, through a domain, etc.), it is difficult to perform supervision over them.

Threat related to variability in the implementation of due diligence measures:
There may be variations in the application of due diligence measures by gambling operators. This difference may arise, in particular, in the implementation of additional due diligence measures, of which the law has left relatively large freedom of interpretation to the obliged entity. This is also confirmed by the survey responses, which show that market participants use very different methods to identify the origin and purpose of funds in higher-risk cases. If in this case more than half of the market participants apply gathering additional data from the customer, then, for example, only two market participants have listed information from public databases and two more from paid databases. The following measures are also listed in the answers for the open question: at the time of the survey, one market participant's customer is banned from gambling and payouts, one market participant has asked for a copy of passport and proof of address, five market participants have asked for all financial information (credit statement, savings statement, income statement, company income statement), four market participants have carried out an internet/social media inquiry, two market participants have mentioned requesting information from third parties, etc.

Threat related to high-risk customers:
The share of non-resident customers in gambling operators is higher than average. However, market participants also pay close attention to threats when implementing due diligence measures to riskier customers and riskier customers are subjected to additional due diligence measures (see the section on the threat associated with the application of due diligence measures), which reduces the threat from high-risk customers. It is also important to note that gambling customers can only be natural persons, which excludes certain high-risk customer profiles (such as embassies, virtual asset service providers, financial services companies, non-profit organizations, etc.). There is also a possibility that in the absence of sufficient control, natural persons use bank cards of legal entities.

The threat associated with the use of virtual currencies:
The problem is topical, as various virtual currencies are gaining more and more widespread handling, and as of December 2020, the Tax and Customs Board has also received several inquiries regarding the possibility of using virtual currencies in the gambling sector. The Tax and Customs Board has given its consent on one occasion so far. Different virtual currencies have different levels of anonymity, and their use can make it difficult or impossible to trace the origin of funds.

The threat of playing with unverified bank and credit cards:
About two-thirds of the responding market participants[18] have encountered attempts to use stolen credit cards for betting in the course of their activities, which indicates the threat that someone else's bank or credit card may be used for gambling.

[18] 12 market participants or 63.16%.

10.4.1.2. Risk awareness

Management commitment and leadership role

The results of a survey of market participants in the sector show that the sector's awareness of anti-money laundering is rather high. All interviewed market participants have created guidelines for the prevention of money laundering in a company or corporation and established rules of procedure for the prevention of money laundering, which can be attributed to the high level of regulation of the field and the obligatory status of all market participants within the meaning of the MLTFPA. All market participants who responded to the survey have also confirmed that the company has developed a methodology and/or guidelines for reporting in case of a suspicion of money laundering or an unusual transaction. Just under half[19] of the respondents have confirmed that the guidelines are needed in practice to submit a report to the FIU.

Reporting statistics of the sector support the feedback received from the survey. The sector is satisfactorily fulfilling its reporting obligation: notifications are sent both on suspicion of money laundering and on the basis of the amount of cash in transaction.

Table 59. The reporting statistics in gambling sector for 2017-2019

2017	**Casinos**	**Remote gambling operators**	**The most active market participant**
CTR	282	-	274
STR/SAR	1	2	1
UTR	-	-	-
TFR	36	-	36
Into the file	66	-	66

2018	**Casinos**	**Remote gambling operators**	**The most active market participant**
CTR	221	-	213
STR/SAR	4	-	2
UTR	2	-	2
TFR	52	-	52
Into the file	50	-	50

2019	**Casinos**	**Remote gambling operators**	**The most active market participant**
CTR	**159**	**-**	**138**
STR/SAR	7	2	3
UTR	6	-	6
TFR	75	-	75
Into the file	55	-	53

2020	**Casinos**	**Remote gambling operators**	**The most active market participant**
CTR	75	-	50
STR/SAR	23	11	14
UTR	3	-	2
TFR	-	-	-
Into the file	13	-	12

[19] 8 market participants or 42.11%.

In the tables, "CTR" refers to amount-based reports, "STR/SAR" to suspicious transactions, "UTR" to unusual transactions, and "TFR" to unusual transactions involving risk areas of terrorist financing. "To the file" means that the received messages are placed in the in-depth analysis file and used for in-depth analysis of a case.

Comparing the feedback received from the survey with the reporting statistics of the sector, the fulfillment of the reporting obligation can be considered satisfactory. The classification of notifications shows that the main reasons for sending reports are formal parameters (transaction over a threshold or related to risk countries). There are significantly fewer suspicion-based reports. In the practice of the FIU, there have been no cases where the reason for sending the material to the investigative bodies was a report sent from the gambling sector. However, there have been cases where the information contained in sector reports has been used in the analysis of other cases where a link to the sector has been identified during the analysis.

On the other hand, statistics show that more than 90% of reports are sent by a single service provider, suggesting that the sector as a whole may not be evenly covered. This is also indicated by the results of the above-mentioned survey - although all surveyed market participants have confirmed that the company has developed a methodology and/or instructions for reporting in case of suspicion of money laundering or unusual transaction, then, in practice, less than half of the market participants have used the instructions in practice to report to the FIU.

New and planned amendments to the law are discussed in the Market Participants Advisory Committee, where a representative of the Estonian Gaming Operator Association is also represented. On the other hand, just under half of the market participants who responded[20] had the opinion that there are sectoral round tables, discussions, or other forms of cooperation on anti-money laundering, although mostly[21] they, in turn, find that the roundtables and discussions have been of practical benefit to the company - for example, one can ask questions there, discuss proposals for amending the law, etc. This suggests the possibility that part of the sector - especially the part not belonging to the professional association - may be less informed and involved in terms of awareness and cooperation.

The vulnerability of the gambling sector is rather low in terms of management commitment and leadership and employee integrity. The vulnerability is reduced by training employees[22]. Many of them have trained all or a large part of their staff in the last three years. The requirement to train employees also arises from the law itself.[23] The majority of responding market participants consider that the company's employees have a good level of understanding of the obligation to report suspicious transactions.[24]

The fact that, according to the law, a gambling operator must ensure that a person punished for a criminal offense is not responsible for organizing gambling, making decisions on the right to participate in gambling, or carrying out supervision of gambling also contributes to ensuring the integrity of employees.[25] At least once a year, the Tax and Customs Board conducts a background check of the criminal record for all employees of gambling companies.

Brief summary

Analyzing the responses to the survey conducted among market participants and the statistics of submitting notifications to the FIU, it can be said that the risk awareness of money laundering in the sector is rather acceptable. In addition to the materials prepared by the legislator and the FIU, market participants have developed internal guidelines and rules of procedure, and employees are trained regularly, with the majority of responding market participants assessing highly the awareness of their employees. According to the statistics submitted to the FIU, the notification obligation in the sector is satisfactorily fulfilled, but the fact

[20] 8 respondents, i.e., about 42%.
[21] 7 respondents or about 37%.
[22] 14 market participants, or about 74%, have answered that they send employees for training.
[23] § 14 (6) of the MLTFPA.
[24] 15 market participants who responded to the survey, i.e., about 79%.
[25] § 33 (1) 3) of the Gambling Act.

that the majority of notifications are made by one active market participant may indicate the need to raise the level of awareness among smaller market participants in the sector. The number of notifications transmitted by remote gambling operators is also low. The results of the survey suggest that part of the sector - especially the part not belonging to the professional association - may be less informed and involved in terms of awareness and cooperation.

10.4.1.3. Legal framework and control

Quality of supervision

The gambling sector is regulated in great detail, as in addition to the requirements arising from the MLTFPA, Gambling Act also sets strict requirements for operating in the sector. When qualifying for an activity license for the organization of gambling and an operating permit for gambling games, great attention is paid, in addition to the technical and financial aspects, also to the reputation and credibility of the organizer's owners and members of the management body (so-called "fit-and-proper" requirements), moreover, conditions and exclusions are set for the personnel responsible for conducting gambling.

In addition to the regulation established at the level of the law, the law provides[26] the FIU has the right to issue advisory guidelines to explain AML/CFT legislation, whereas the law stipulates that the FIU shall issue guidelines regarding the characteristics of suspicious transactions,[27] and guidelines regarding the characteristics of transactions suspected terrorist financing[28]. In practice, the FIU has issued the following guidelines[29], which also apply to gambling operators:

- Form of a report submitted to the FIU
- Guidelines for submitting a report to the FIU
- Guidelines on the characteristics of suspicious transactions
- Recommendations of the FIU for managing the threats arising from the activities of obliged entities
- Recommendations of the FIU for drafting rules of procedure and internal control rules
- Guidelines of the FIU for application of international financial sanctions

Neither regulators nor supervisors have developed sector-specific guidelines. However, according to the survey, all respondents have developed internal rules procedures for preventing money laundering. More specific guidelines at the national level taking into account the specificities of the sector could be considered.

The role of the regulatory, and supervisory body is performed by the TCB, which has four full-time supervisory officials. The rights and competence of the TCB in exercising supervision over the gambling sector are extensive and in full compliance with the need to ensure the effectiveness of regulations in the sector. The FIU also has supervisory competence, which supervises compliance with the requirements of the MLTFPA. It should be noted that the FIU supervises obliged entities on a threat-based approach, but so far, the emphasis has been mainly on financial institutions.

The Estonian Gaming Operator Association, which includes about half of the market participants, has regulated its activities with the articles of association. Although the article of association does not explicitly address issues related to the prevention of money laundering and terrorist financing, it refers to cooperation with state, municipal, scientific and cultural authorities, civil society organizations and movements, creative associations, as well as other authorities, businesses, and individuals interested in the activities of the association. The statutes also list the organization of training as one of the main activities. Given the level of detail of state regulation, the ethical standards of this sector can be assessed as rather high in the light of the above.

[26] § 56 (1) of the MLTFPA.
[27] § 56 (2) of the MLTFPA.
[28] § 56 (3) of the MLTFPA.
[29] https://www.politsei.ee/et/juhendid

Brief summary

In general, the level of regulation and supervision in the sector is high. At the level of the law, comprehensive requirements have been set for gambling operators, the FIU has also prepared guidelines, and all market participants have internal rules, for which the obligation to compile and the requirements also arise from the law. The role of the supervisory, and regulatory body is performed by the TCB, which has four full-time supervisory officials focused on the sector. The FIU supervises the obliged entities on a risk-based approach, and so far, the emphasis has been mainly on financial institutions. The professional association of the sector is the Estonian Gaming Operator Association, which includes about half of the market participants and whose ethical standards can be considered high.

Effectiveness of compliance control systems and reporting

The threat-based approach is extensively set out in MLTFPA.[30] Although there are no direct legal requirements for investments by operators, each operator must establish and implement an appropriate money laundering risk mitigation process, which may include, but is not limited to, IT systems and mechanisms to identify unusual or suspicious transactions. Market participants vary in size, volume, and business model and implement measures and investments in technical solutions according to their operating model. Most market participants have responded that they have systems in place to identify suspected money laundering transactions. The majority of market participants have also confirmed that the company has a system on the basis of which the customer's risk level is determined.

Half of the respondents have explained that they invest in technological risk management solutions. The following systems are listed as such solutions:

- IT solutions;
- automatic monitoring system;
- paid databases;
- use of programs;
- solutions for risk assessment.

The effectiveness of market participants' compliance control systems can be assessed on the basis of the results of the surveys as follows:

- The monitoring systems of market participants are either automated or semi-automated; the monitoring systems of smaller market participants are solved either manually or purchased by the service provider, and it depends on the volume of service provision.
- The members of the sector with the largest market share have systems for detecting money laundering indicators; a risk-based approach is applied.
- Most market participants use a system that allows for a risk-based calculation of the customer's risk level.
- More than half of market participants invest in technological risk management solutions, such as automation of the compliance system, implementation of programs, or IT solutions to mitigate risks.

Brief summary

In general, the effectiveness of the sector's compliance control systems and reporting can be considered above average.

Quality of the due diligence framework applied in regard to the customer

The general due diligence measures applied to the customer derive from the MLTFPA, according to which the obliged entity applies at least the following due diligence measures: identification of a customer or a person participating in an occasional transaction and verification of the submitted information, identification, and verification of a representative and their right of representation, identification of the beneficial owner and taking measures for identification thereof to the extent that allows the obliged entity to make certain that it knows who the beneficial owner is and understands the ownership and control structure, understanding of business relationship, an occasional transaction or operation, gathering information on whether a person is a

[30] MLTFPA Chapter 2 - Money laundering and terrorist financing threat management.

politically exposed person, their family member or a person considered to be close associate, and monitoring of a business relationship.

In addition to MLTFPA, the Gambling Act also sets requirements for customer identification. The organizer of a game of chance is required to identify the persons entering the gaming location. Upon identification, the following information shall be registered: forename and surname; personal identification code, in its absence date of birth; the name, serial number, date, and place of issue of the identification document; the time and date of arrival in the gaming location for games of chance. In order to register this information, a person wishing to enter the gaming location shall present an identification document. A copy of the page of the identification document containing personal data shall be made, and the data shall be entered in an electronically maintained database. Before a person enters a gaming location, the gaming organizer shall verify the data on persons who have visited the gaming location in the electronically maintained database on the basis of the identification document submitted for identification and enter in the database the time and date of the person's arrival at the gaming location. With regard to remote gambling, MLTFPA stipulates that in order to organize remote gambling, the gambling operator must ensure the identification of each player.

The main vulnerabilities identified during the survey in assessing the quality of the due diligence framework applicable in regard to the customer are the identification of high-risk customers, in particular politically exposed persons.

Most of the responding market participants[31] confirmed that the company has a system for determining the customer's risk level. In contrast, only a quarter[32] of respondents have found that the information needed to identify and verify high-risk customers is readily available; the rest either felt that such information was not readily available or could not provide an assessment. Only two respondents to the survey found that access to the information needed to identify and verify resident politically exposed persons is available and easy. The rest could not answer or considered access to information difficult or even inaccessible. More than half of the responding market participants considered that information on foreign politically exposed persons is available. It follows from the above that it is difficult to identify politically exposed persons, as there are no relevant available national, international, or other databases that are necessary for the effective and efficient fulfillment of the requirement.

The survey also shows that the Estonian information systems used to verify customer data are often not considered thorough and reliable.[33]

Brief summary

The Quality of the framework of due diligence measures applicable regarding a customer can be considered good, as both MLTFPA and the special law set requirements for due diligence measures and customer identification, although information on high-risk customers who are politically exposed persons is difficult to access in practice.

10.4.1.4. Sector-specific risk assessment with the Quality of sector-specific controls

The following vulnerabilities and their mitigation have been identified in the analysis and assessment of sector-specific risks:

- **Prevention of the collection of fabricated gambling winnings**

When organizing gambling, the gambling operator is obliged to ensure sufficient measures to identify persons who use technical aids, which enable creating an advantage for themselves or others in gambling and to impede the randomness of determining the outcome of a game and exclude the participation of such persons in gambling;[34] The operator of the game of chance or toto must ensure internal and external video surveillance

[31] 15 market participants, i.e., about 79%.
[32] 5 market participants, i.e., about 26%.
[33] 4 market participants or 21.05% always considered the information in these information systems to be reliable.
[34] § 33 (1) 6) of the Gambling Act.

of the gaming location for the games of chance or toto. Recordings must be kept for at least 14 days from the moment of recording.[35] The above does not apply to a gambling location on a ship carrying passengers registered in the Estonian ship register.

Market participants have implemented systems to control prizes. For remote gambling, there are comprehensive logs of customer transactions and game history. In land-based casinos, it is difficult to falsify gaming tickets, as payouts will not be made unless there is confirmation of the prize in the system. In practice, there are no cases at the largest operator when this has been tried.

- **Identification of cases where casinos are used as financial intermediaries**

Casinos cannot be used as financial intermediaries, as the law prohibits a gambling operator from engaging in anything other than gambling. In the case of remote gambling operators, additional protection is that, according to the Gambling Act, payouts can only be made to the same current account from which the player has made a payment to the gambling operator's account in order to place bets on gambling.[36] In land-based casinos, the hall has trained staff whose purpose is to monitor visitors and their gaming activities.

- **Detection of the use of illegal funds for gambling**

At the level of the law, a due diligence requirement and a customer monitoring requirement are prescribed. The Gambling Act stipulates that in order to organize remote gambling, the gambling operator must ensure that withdrawals are made only to the same current account from which the player has made a payment to the gambling operator's account in order to place bets on gambling. Market participants have implemented risk management, high-risk customers, and suspicious transaction monitoring systems.

Approximately one-third of the responding market participants have identified cases in the course of their activities since 2017 where there is a suspicion that bets are made on gambling with money obtained by criminal means.[37] Since, in the case of remote gambling, transactions are carried out by credit and payment institutions, then, if illicit money is used, it should, in fact, have been detected and controlled at a previous stage (at the level of the credit or payment institution), as is the case, for example, with card payments on the land. In land-based casinos, the biggest risk factor is cash, the share of which is decreasing, and the corresponding cash risk does not exist in the case of remote gambling.

- **Identifying the purchase of a prize from a legitimate customer**

This threat does not exist in remote gambling, as the prize can only be paid out to the account of the winning player. In the case of land-based casinos, the operators have drawn up guidelines, and staff is trained on how to detect and identify such activities. In terms of technical solutions, such activities are partly observable. Most of the[38] responding land-based operators have not encountered attempts by customers to buy gaming chips from other players at a price higher than the nominal value.

- **Identification of loan sharks**

The Penal Code criminalizes unlicensed and prohibited economic activities.[39] Institutions granting loans must be licensed by FIU or FSA. Market participants have a due diligence obligation requiring them to have risk management, high-risk customer, and suspicious transaction monitoring systems in place. Land-based casinos have cameras. Part of the due diligence obligation is that the customer must be able to explain the origin of his or her money if the gambling operator has requested it in accordance with its rules of procedure and risk-based approach. The threat of loan sharks is rather low in the gambling sector, especially given the fact that there are many legal lenders with more favorable conditions in the market.

[35] § 37 (14) of the Gambling Act.
[36] § 53 (1) 6) of the Gambling Act.
[37] 6 market participants, i.e., about 31.58%.
[38] 3 market participants or 75% of 4.
[39] § 372 of the Penal Code.

- **Preventing money laundering by purchasing game tokens and then redeeming their value by money transfer; preventing money laundering from taking place by purchasing tokens from "clean" players at a higher price**

There is no such threat in the case of remote gambling. The Gambling Act stipulates that in order to organize remote gambling, the gambling operator must ensure that withdrawals are made only to the same current account from which the player has made a payment to the gambling operator's account in order to place bets on gambling. Land-based managers have implemented internal mechanisms for monitoring suspicious transactions and risk management, and training is provided. In the course of their activities, on the basis of the questionnaire, 1 out of 4 market participants has encountered attempts to buy gaming chips for cash and then realize them by money transfer or attempts to buy gaming chips from other players at a price higher than the nominal value.

- **Preventing money laundering by pooling prizes and cash into one casino prize**

There is no such threat in the case of remote gambling, as it is cash. In the case of remote gambling, one can also see what the prize is and what the deposit is. According to the questionnaire, in the course of their activities, 1 out of 4 market participants has encountered attempts to present prizes and cash as one and the same casino prize. In the case of land-based casinos, the machines do not dispense cash but tickets. It is questionable whether land-based casinos can distinguish whether the ticket issued has been played with.

- **Prevention of money laundering in casinos through the deposit box service**

There is no such threat in the case of remote gambling. According to the information available and the results of the surveys, it appears that no land-based operator offers a safe deposit service. However, it must be stated that the law does not directly impose such a restriction on the activities of land-based casinos.

- **Prevent money laundering by purchasing a large number of "casino gift cards"**

According to the results of the survey, no market participant offers gift cards.

- **Prevention of money laundering through gambling against an accomplice/intentional loss**

In the course of their activities, about a quarter[40] of respondents have encountered attempts to place bets against fellow players in order to lose deliberately. It can occur in so-called peer-to-peer games, such as poker. The threat exists for both remote gambling and land-based casinos. Due to the requirements of the law, each operator has an obligation to mitigate the threats applicable to its business model, including implementing measures that enable the threats of peer-to-peer games to be mitigated. Monitoring by remote gambling operators is divided into a system level and a software provider level, wherewith automatic formulas non-standard moves, and behavior are searched for. Also, not all operators offer peer-to-peer gaming products. So-called "cash games"[41] are used in two land-based gambling companies. In the "cash games" of the largest operator, gaming means (chips, plaques) are sold for cash and tickets. At the "cash game," the game is conducted by a dealer, supported by an inspector and a pit boss if it is necessary to take additional measures at the table to ensure compliance with the rules (incl. to prevent money laundering) during the game. The monitoring service monitors the activities of the "cash game," looking for psychological indicators as well as other types of collusion.

- **Prevention of placing bets with parallel 1: 1 winning ratio**

Where gambling is carried out for the purpose of money laundering, low-bet, and low-risk games may be used, such as bets with a 1 :1 winning ratio in roulette. Approximately one-third of market participants have blocked parallel cash bets in the course of their activities (e.g., 1: 1 winning ratio bets in roulette).[42] It is important to note that not all market participants offer a betting service such as toto or roulette. Market participants whose business model includes products where it is possible to bet in parallel 1:1 are obliged to

[40] 5 market participants or 26.32%.

[41] To clarify: the difference between poker and the "cash game": the gaming means used in a poker tournament have no monetary value. Gaming means used at "cash games" have a monetary value. An additional difference is that poker is played peer-to-peer or with each other, but a "cash game" is played against the casino.

[42] 6 market participants or 31.58%.

implement appropriate risk mitigation measures, including monitoring the making of such bets and notifying the FIU in case of a suspicious customer or transaction.

- **Prevention of money laundering in online gambling, where money is wagered as part of a gambling transaction, and then a payout is made as a prize**

The Gambling Act stipulates that in order to organize remote gambling, the gambling operator must ensure that withdrawals are made only to the same current account from which the player has made a payment to the gambling operator's account in order to place bets on gambling. All customer activities, including bets, payments, and prizes, are also logged as part of remote gambling. Therefore, the risk of money laundering in this form is not relevant.

- **Preventing money launderers from using casinos to exchange low-denomination banknotes for high-denomination banknotes**

There is no such threat in the case of remote gambling. There is a corresponding threat in land-based casinos, but due to the requirements of the law, each operator has an obligation to mitigate the threats applicable to its business model, including implementing measures to monitor the respective transactions.

- **Preventing the laundering of the proceeds of stolen credit cards in gambling**

Approximately two-thirds of market participants have encountered attempts to use stolen credit cards to bet.[43] The security of bank and credit cards has been developed by credit institutions, which means that in cases where card data has been copied, it is virtually impossible for the gambling operator to intervene. However, land-based casinos have no obligation to verify if the bank and credit cards used for playing belong to the player, so it is theoretically possible that someone else's bank card may be used for playing.

- **Preventing the use of casinos to convert large amounts of foreign currency**

There is no such threat in the case of remote gambling due to the lack of cash transactions. As of December 2020, foreign exchange is offered by only one land-based service provider, which allows the purchase of gaming means for the currency, but the currency exchange takes place through a currency exchange service provider.

- **Identification of customers using forged identification documents**

According to the answers to the questionnaire, just under half[44] of the market participants have indicated that in the course of their activities, they have encountered attempts by customers to use forged identity cards. The obligation to identify a person arises from both MLTFPA and the Gambling Act. When analyzing the results of the survey, it is also important to keep in mind that the use of forged documents may be due to the fact that the customer is on a self-exclusion list but still tries to access the gambling environment. The threat of using forged documents is mitigated by the requirement to identify the person.

- **Identification of employees who work with customers to prevent the detection of money laundering transactions**

None of the responding market participants has identified a situation where the company's employee has cooperated with customers. Most market participants[45] have stated that they carry out background checks on staff. More than half of the respondents[46] have explained in response to the survey that they also carry out an assessment of the reliability of employees during the employment relationship.

- **Identification of structuring, restructuring, or transactions below the control threshold for money laundering purposes**

Two market participants[47] have, in the course of its activities, identified attempts to structure, redistribute or disguise transactions with the presumed purpose of avoiding the application of due diligence measures

[43] 12 market participants or 63.16%.
[44] 8 market participants or 42.11%.
[45] 17 market participants or 89.47%.
[46] 10 market participants or 52.63%.
[47] 2 market participants or 10.53%.

prescribed in the MLTFPA. The gambling operator shall apply due diligence measures at least in the event of a payout of the prize, placing a bet or both if the amount given to or received from the customer is at least EUR 2000 or the equivalent in another currency, regardless of whether the financial obligation is met in a lump sum or by way of several linked payments over a period of up to one month.

Brief summary

The main vulnerabilities in the sector are, in particular, match-fixing, including deliberate losing, as well as the purchase of winnings, tokens, and tickets, for example, money laundering through the purchase of chips and their subsequent redemption by money transfer, money laundering through the purchase of chips from "clean" players at a higher price, money laundering through playing with an accomplice/ intentional loss, cases where money launderers use casinos to exchange low denomination banknotes for high denomination banknotes, laundering of proceeds from stolen bank cards, as well as misuse of cards in other ways (such as bank cards of legal entities). As a countermeasure, market participants implement internal control mechanisms (both fully automatically and semi-automatically) and train their employees to recognize such schemes. Some of the listed threats occur only in land-based casinos, others only with individual service providers (e.g., toto, roulette). When determining the level of threat in a sector, it must be borne in mind that many sector-specific money laundering risks do not apply to remote gambling operators due to the lack of cash use and physical gaming means and location. Therefore, the level of vulnerability to sector-specific risks in the gambling sector must be considered average/low.

10.4.1.5. Sector-specific risk assessment in regard to additional controls

In the framework of this risk assessment, the need to open a further discussion on the possibilities of gambling operators to use virtual assets has been analyzed. The current law does not regulate whether gambling operators can allow players to use virtual assets. According to the current Gambling Act, the gambling operator must identify the person who owns the bank account, which has been interpreted in practice by the regulatory authority as meaning that it is necessary to identify who owns the virtual asset wallet and no one else may make payments from the wallet. However, when analyzing the issue, it must be borne in mind that the different virtual assets have varying degrees of anonymity and that, in some cases, the owner of the wallet cannot be identified or verified. In practice, the regulator has recently received such a request, and there is reason to believe that the issue will play an increasingly important role in the future, which is why it calls for further analysis. The discussion should be led by regulators and supervisors (including the TCB and FIU). The professional association and market participants can then take a position.

The need for mandatory reporting of large bets in land-based casinos has also been analyzed. In essence, a possible scheme is to claim that large sums have been paid off when in reality, this has not been done. There is no such reporting obligation at the statutory level but only a general due diligence obligation, so the introduction of such a reporting obligation should also be considered at the statutory level.

Brief summary

The unclear position of virtual assets and the lack of mandatory reporting of large bets can be seen as the main vulnerabilities in the assessment of sector-specific risks. As the current Gambling Act requires a gambling operator to identify the person who owns a bank account, which has been interpreted in practice by the regulatory authority so that it is necessary to identify who owns the virtual asset wallet and cannot make payments from someone else's wallet, the possible vulnerability is not yet particularly high, but definitely needs further follow-up. Concerning the mandatory reporting of large contributions, in addition to money laundering, it can also play a role in various tax frauds as possible predicate offenses, which is why this issue also needs further analysis. On the other hand, statutory due diligence measures are applied (a gambling operator applies due diligence measures at least in the case of paying out prizes, placing bets, or both if the amount given to or received by the customer is at least 2000 euros or the equivalent in another currency, regardless of whether the financial obligation is fulfilled in a single payment or by the way of several linked payments over a period of up to one month) also the potential vulnerabilities resulting from this additional control.

10.4.1.6. Quality of response to threats identified in previous evaluations

The sector was not separately assessed under the previous NRA 2015, but the sector of designated non-financial businesses and professions (*DNFBPs*) was assessed more broadly.

It was found necessary to analyze the adequacy of the obligations of the toto and lottery operators in taking over AMLD IV and to consider whether it would be expedient for Estonia (for example, from a certain prize amount or acceptance of a bet) to bring the toto and lottery operators to the circle of obliged entities of MLTFPA. The mentioned proposals were addressed, and since the adoption of MLTFPA, which entered into force in 2017, the entire gambling sector in Estonia is now obliged entities, except for the operators of a commercial lottery[48].

In this sector, Moneyval has found in the 4th round of evaluation that the regulation of casinos in MLTFPA is in line with the Directive, and no further recommendations were made to the sector.

In the case of SNRA 2017/2019, it was found for this sector that there is a significantly higher risk of money laundering for certain gambling services across Europe. In the case of land-based betting and poker, this was attributed in particular to ineffective controls, either due to the fact that these activities by their very nature involve a large number of fast, anonymous, and often cash-based transactions or a peer-to-peer element without proper supervision. In the case of online gambling, the high risk derives from the large volumes of transactions and the non-face-to-face element. In the case of online gambling, anonymous transactions are possible, which is alleviated at the same time by the fact that the transactions can be monitored. Lotteries and gaming machines involve a moderate RP/TR risk. In the case of lotteries, a certain level of control has emerged in relation to high prizes. Although casinos are an inherently high risk, their inclusion in the RP/TR framework since 2005 has mitigated the risks. Land-based bingo is considered low in terms of RP/TR risks due to relatively low stakes and prizes.[49]

In the gambling sector, it was considered that, for gaming machines, supervisors should provide clearer guidance on the risks associated with video lotteries. With regard to online gambling, the responsible, competent authorities should also establish programs to raise the awareness of online gambling operators about emerging risk factors that may affect the vulnerability of the sector. These include the use of anonymous e-money or virtual assets and the emergence of unlicensed online gambling operators; FIUs should provide further feedback on the quality of STRs, opportunities for improving reporting and the use of the information provided and taking into account the specificities of the gambling sector in the development of standardization of STR/SAR templates at EU level. For betting, Member States should, in addition to staff and compliance officers, design mandatory training for betting service providers focusing on an appropriate risk assessment of their products/business model.[50]

The SNRA 2019 report found that in many Member States, FIU feedback to the obliged entities is still incomplete, despite the existence of national rules and sectoral guidelines. The recommendation to strengthen cooperation between competent authorities and obliged parties and to provide additional training was partially maintained.[51]

With regard to the gambling sector, it was also considered that competent authorities should put in place programs to raise awareness among (Internet) gambling operators of emerging risks that may affect the sector's vulnerability, including the use of anonymous e-money and virtual assets and the emergence of unlicensed gambling operators. Feedback from FIUs on the Quality of suspicious transaction reports would

[48] A commercial lottery is a classic or instant lottery organized under national law by a supplier of goods or services to promote the sale of goods or services or to advertise goods, services or their supplier. The right to participate in a commercial lottery is acquired together with the acquisition of goods or services. Requiring additional financial obligations from a participant in a commercial lottery is prohibited. Thus, at the legislative level, the approach chosen is a form of gambling organized by dealers, which in many countries is not regulated as gambling at all, so the money laundering risks of commercial lottery operators are thus essentially the risks of dealers, not the threats of gambling operators.

[49] SNRA 2017, p. 5.

[50] SNRA 2017, pp. 19-20.

[51] SNRA 2019, p. 17

improve reporting and the use of the information provided. FIUs should take into account the specificities of the gambling sector when developing standard reporting templates for suspicious transactions at the EU level. Member States should provide adequate training focusing on risk assessment of relevant products/business models for the employees responsible for the staff and compliance control and retailers, and additional guidance on the concept of "multiple related operations" should be provided to obligated parties.[52]

The following proposals were made to the Member States in the gambling sector under SNRA 2017/2019:
1) To the competent authorities
• Member States should improve cooperation between relevant authorities in order to better understand the risk factors associated with betting activities and to be able to provide effective guidance.
• Member States should ensure regular cooperation between the relevant authorities and betting operators. Better cooperation will focus on:
- Strengthening the detection of suspicious transactions and increase the number and quality of STRs;
- Organization of training for the staff and officers responsible for compliance control, paying particular attention to the threats of infiltration or acquisition of shareholding by organized crime groups and risk assessments of products/ business models that need to be regularly reviewed;
- Supervisory authorities will provide clearer guidance on the fight against RP/TR, on CDD and STR requirements, and on how to define the most important indicators for detecting money laundering risks.
-to ensure that FIUs provide feedback to betting operators on the quality of STRs, ways to improve reporting, and the use of the information provided, preferably within a specified timeframe;
- Development of standardized STR/SAR templates at the EU level, taking into account the specificities of the gambling sector.

2) For the sector
• Member States should ensure that betting operators regularly train staff and officers responsible for compliance and retailers, paying particular attention to the risks of infiltration or acquisition of shareholding by organized crime groups and risk assessments of products/ business models that need to be regularly reviewed;
• Member States should ensure that betting operators promote player cards or use electronic identification systems to facilitate customer identification and restrict the use of cash, and use real-time tracking systems to detect suspicious transactions at the point of service;
• Member States should ensure that betting operators appoint an (on the premises) official dealing with prevention of money laundering if this is not already the case;
• Member States should ensure that betting operators promote a systematic risk based CDD for winners and apply a lower threshold for prizes corresponding to the CDD (currently EUR 2000 in accordance with Article 11 (d) of Directive (EU) 2015/849).[53]

In this context, it is necessary to mention that in Estonia the cooperation between the relevant authorities (the Tax and Customs Board, FIU) and between gambling operators works well. The share of STRs has increased over time. The organization of training for staff and officers responsible for compliance is on the rise. The FIU, as the supervisory authority, has prepared various guidelines and started to provide feedback on the quality of STRs, which is planned to be done more and more in the coming years. There are also increasing plans to provide training for market participants, especially considering, for example, the fact that, according to the statistics on the submission of STRs, most of them are received from one gambling operator.

With regard to the guidelines issued to the sector, the following should be noted. According to the survey, market participants are constantly conducting staff training. The share of cash has decreased, and the operators have increasingly moved to the loyalty card system. Approximately half of the responding market participants have responded to the survey that they use semi-automatic or fully automatic monitoring systems to identify money laundering risks. The largest land-based casino has had a player card system in place for many years in order to electronically identify customers. There are no uniform guidelines for the sector to carry out due

[52] SNRA 2019, p. 20
[53] SNRA 2017 and 2019 annexes.

diligence measures, which the umbrella organization could organize in the form of round tables or training in cooperation with regulators.

10.4.2. Conclusion

Table 60. Level of money laundering vulnerability in the gambling sector

Sector	Level of money laundering vulnerability at the sectoral level	
Gambling sector	2.43	**low**

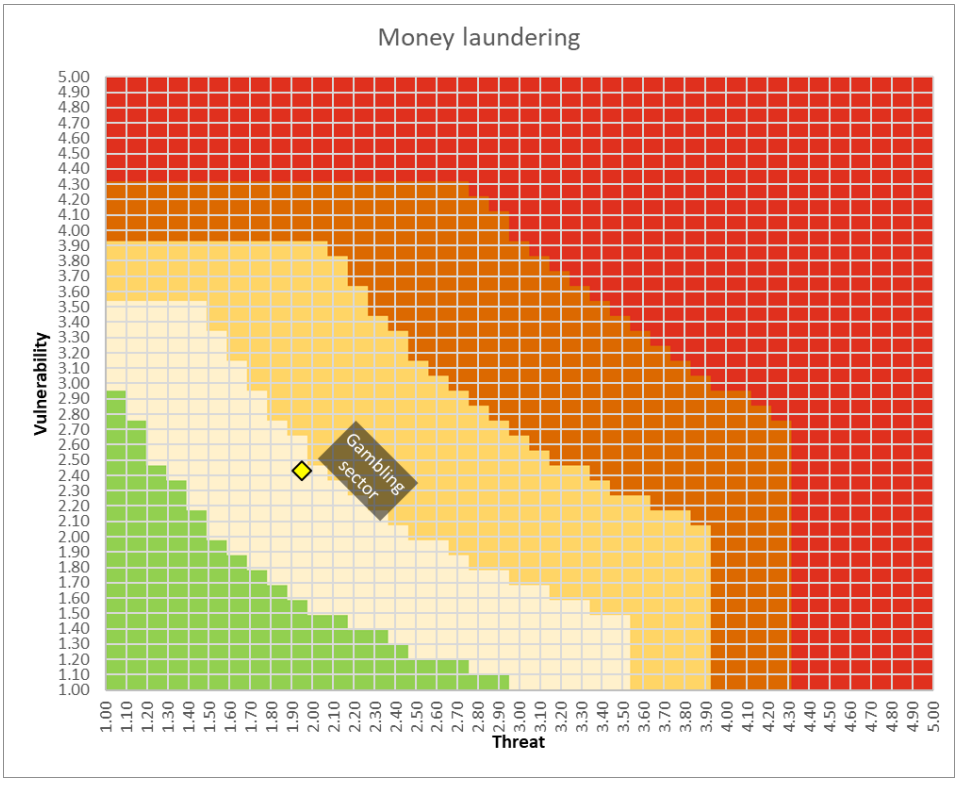
On a scale of 1-5, the vulnerability score of the gambling sector is 2.43 or **low** from the aspect of money laundering.

The strengths of the sector include good supervision, the legal framework, and the commitment of management.

The most vulnerable areas are the efficiency of compliance systems and reporting and the quality of the due diligence framework of customer control. One of the weaknesses has been identified as access to identify individuals (especially high-risk customers such as PEPs). This aspect needs to be addressed at the national level.

Due to the low level of vulnerability of the sector, it is unlikely that there is a need to strengthen regulation or supervision of the sector for this reason, and the focus should be on maintaining the level achieved. Thus, the focus could be on developing more sector-specific guidelines and conducting training and round tables.

Figure 17. Heat map of the money laundering risk level of the gambling sector



Summary

The risk level of the sector in terms of money laundering is **low**, which means that the risk and its consequences must be accepted, and no specific measures are considered necessary. The sector may apply due diligence measures in a simplified manner.

10.4.3. Risk management strategy

10.4.3.1. Risk mitigation measures at the national level

Based on the results of the risk assessment, the following suggestions are made to improve the situation at the national level:

- To carry out an analysis of whether the use of virtual assets by gambling operators should be allowed. In this context, it is also possible to consider, for example, distinguishing between virtual assets on the basis of anonymity;
- To establish a database/register of politically exposed persons;
- To organize sector-specific training and discussions on money laundering typologies and scenarios in cooperation with the FIU;
- To establish a sector-specific guideline on what constitutes a high-risk customer criterion (except for the statutory 2000 euros);
- To establish more sector-specific guidance on a risk-based approach;
- To consider allowing obliged entities in the gambling sector to make a query to the TCB database on whether the person's funds correspond to his or her standard of living and a specific transaction; to consider requiring the existence of an employee/contact person, etc. at the level of the law, analogously to the contact person requirement established for example to credit institutions in MLTFPA;
- To consider introducing a reporting obligation for large bets;
- To collect accurate and comprehensive national statistics (e.g., by sector, etc.) on, inter alia, seizures, and confiscations of assets, predicate offenses, etc.

10.4.3.2. Risk Mitigation measures at the level of obliged entities

Based on the results of the risk assessment, the following proposals are made to improve the situation within the sector:

- To raise awareness through sector-specific training: ECDD framework, sharing of KYC best practices in a professional association
- Development of monitoring systems by obliged entities.

10.4.4. Vulnerabilities of prevention of terrorist financing

10.4.4.1. Exposure to the threat

The threat of terrorist financing in the gambling sector is minimal. With regard to the prevention of terrorist financing, all gambling operators are subject to strict obligations analogous to the prevention of money laundering, including the obligation to apply due diligence, the obligation to provide information based on amount and suspicion, etc. - therefore the aspect of terrorist financing is mostly not considered or analyzed separately in the gambling sector. On the other hand, the use of schemes specific to terrorist financing would be largely ineffective in the context of the gambling sector. Therefore, in practice,[54] an assessment of the threats of terrorist financing has not been found to be practical or appropriate for the gambling sector. For the above reasons, the specifics of terrorist financing have not been largely distinguished in the survey conducted among market participants.

Regarding vulnerabilities specifically in the field of terrorist financing, the survey shows that the majority (89%)[55] of the market participants have indicated that it checks the lists of international sanctions for persons and transactions suspected of terrorist financing or international sanctions. There is a list of countries and territories with a higher risk and a list/database of sanctions that have been made available to operators for risk management. However, only about two-thirds[56] of the market participants considered the sources for

[54] E.g., SNRA 2019.
[55] 17 market participants or 89.47%.
[56] 12 market participants or 63.16%.

identification of the existence of the sanction to be available, whereas around one-fifth[57] has found that these sources are not available. Just under half[58] of the market participants have also explained in their description of their suspicious transaction monitoring system that it allows the identification of transactions related to suspected terrorist financing.

10.4.4.2. Quality of response to threats identified in previous evaluations

The sector was not specifically assessed under the previous NRA 2015, but the sector of designated non-financial businesses and professions (*DNFBPs*) was assessed more broadly.

It was found necessary to analyze the adequacy of the obligations of the toto and lottery operators in taking over AMLD IV and to consider whether it would be expedient for Estonia (for example, from a certain prize amount or acceptance of a bet) to bring the toto and lottery operators to the circle of obliged entities of MLTFPA. The above-mentioned proposals were addressed, and since the adoption of MLTFPA, which entered into force in 2017, the entire gambling sector in Estonia is an obliged entity, except for the operators of a commercial lottery[59].

In this sector, Moneyval has found in the 4th round of evaluation that the regulation of casinos in MLTFPA is in line with the Directive, and no further recommendations were made to the sector.

In the case of SNRA 2017/2019, the sector was not considered in the context of terrorist financing.

10.4.5. Conclusion

Table 61. Level of the vulnerability of terrorist financing in the gambling sector.

Sector	Level of the vulnerability of terrorist financing at sectoral level	
Gambling sector	2.38	**low**

On a scale of 1-5, the vulnerability score of the gambling sector in terms of terrorist financing is 2.38, i.e., **low**.

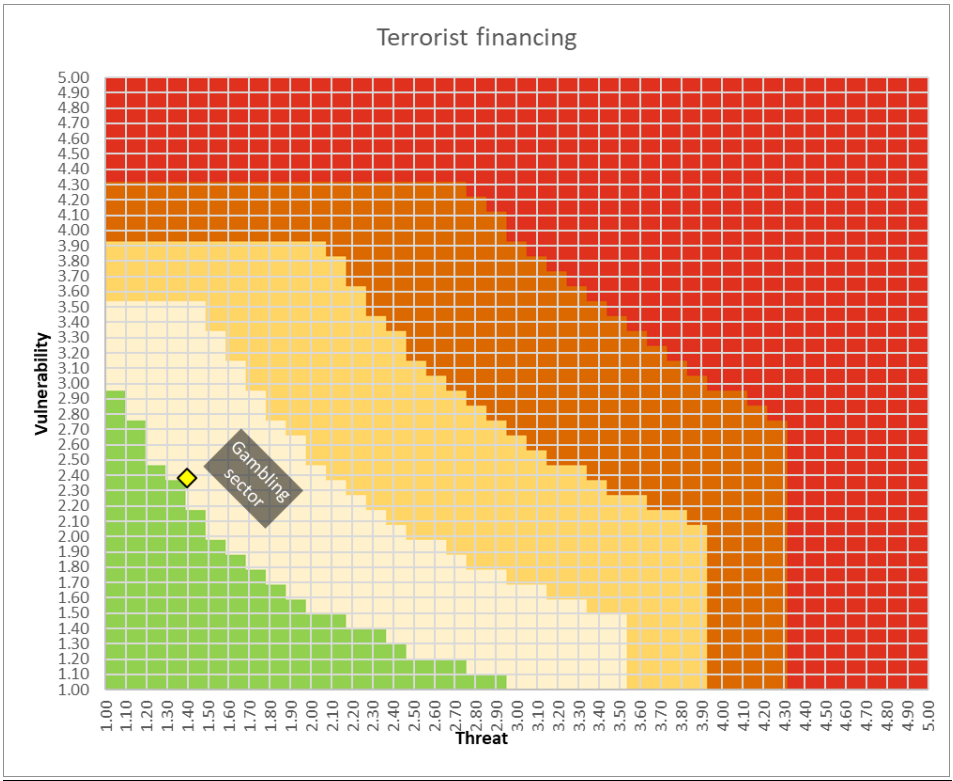
The strengths of the sector include good supervision, the legal framework, and the commitment of management.

The most vulnerable areas are the efficiency of compliance systems and reporting and the quality of the due diligence framework of customer control. One of the weaknesses has been identified as access to identify individuals (especially high-risk customers such as PEPs). This aspect needs to be addressed at the national level.

Due to the low level of vulnerability of the sector, it is unlikely that there is a need to strengthen regulation or supervision of the sector for this reason, and the focus should be on maintaining the level achieved. Thus, the focus could be on developing more sector-specific guidelines and conducting training and round tables.

[57] 4 market participants or 21.05%.
[58] 8 market participants or 42.11%.
[59] A commercial lottery is a classic or instant lottery organized under national law by a supplier of goods or services to promote the sale of goods or services or to advertise goods, services or their supplier. The right to participate in a commercial lottery is acquired together with the acquisition of goods or services. Requiring additional financial obligations from a participant in a commercial lottery is prohibited. Thus, at the legislative level, the approach chosen is a form of gambling organized by dealers, which in many countries is not regulated as gambling at all, so the money laundering threats of commercial lottery operators are thus essentially the threats of dealers, not the threats of gambling operators.

Figure 18. Heat map of the terrorist financing risk level of the gambling sector



Summary

The level of risk in the sector in terms of terrorist financing is **low**, which means that the risk and its consequences must be accepted, and no specific action is considered necessary. Due diligence measures may be applied in the sector in a simplified manner.

10.4.6. Risk management strategy

10.4.6.1. Risk mitigation measures at the national level

Possible mitigation measures at the national level overlap with mitigation measures preventing money laundering.

10.4.6.2. Risk mitigation measures at the level of obliged entities

Possible mitigation measures at the level of obligated parties overlap with mitigation measures preventing money laundering.