CATALOGUE OF

RISK

INDICATORS

2024

Gaming Sector

MINISTERIO
DE ECONOMÍA, COMERCIO
Y EMPRESA

COMMISSION FOR THE PREVENTION
OF MONEY LAUNDERING AND
MONETARY OFFENSES

INTRODUCTION

This document contains a list of risk indicators for money laundering and terrorist financing (hereinafter ML/TF).

The purpose of this document is to assist regulated entities in complying with Law 10/2010 of April 28 on the prevention of money laundering and terrorist financing. Knowledge and use of these indicators can help improve the systems implemented by regulated entities to prevent and detect money laundering or terrorist financing transactions.

The presence in specific transactions of the indicators shown in this list does not necessarily imply the existence of money laundering or terrorist financing, which must in any case be assessed in the corresponding special review to be conducted by the regulated entity. However, the presence of these indicators can help the regulated entity identify the cases to be selected for the special review.

Likewise, the list of indicators provided below, duly adapted to the nature of the regulated entity's activities, may assist the entity in developing its own list of transactions that may be related to money laundering or terrorist financing.

Law 10/2010 of April 28 on the Prevention of Money Laundering and Terrorist Financing, in Article 2.1(p) and (u), designates casinos and gambling operators as obligated entities.

As indicated in the National Risk Assessment approved by the Commission for the Prevention of Money Laundering in 2020, updated in April 2024, this sector carries a **high inherent risk** because it is a sector—particularly casinos—traditionally exposed to dishonest behaviour by both customers and employees, as well as remote gambling. However, the characteristics of the gambling market in Spain make it less vulnerable thanks to factors such as strict prudential regulation, the strict access regime for operators, the monitoring carried out by the operators themselves, their extensive knowledge of AML/CFT regulations, and detailed statistical information on the sector, among others.

These factors, combined with the existence of mitigating measures of a regulatory, supervisory, informational, and awareness-raising nature, lead to the conclusion that we are dealing with a sector of **moderate/low residual risk**; however, the residual risk identified must be assessed differently depending on the type of gaming (with a higher risk attributed to remote gaming).

In this context, the FATF developed a risk-based guide on the casino sector in 2008[1]. Furthermore, in 2009, it published a report on the vulnerabilities of the gaming and casino sector[2]. Meanwhile, the European Gaming Association developed Guidelines on Combating Money Laundering and Terrorist Financing for the European Online Gaming Sector[3].

Finally, in 2022, the European Commission published the third edition of the so-called Supra-National Risk Assessment (SNRA), which provides a systematic analysis of the risks of money laundering and terrorist financing at the European Union level, including, among other sectors, the risks specific to the gambling sector[4].

This Catalogue has been prepared by the Commission for the Prevention of Money Laundering and Monetary Offenses, in the exercise of its functions, with the collaboration of industry associations and with the aim of facilitating compliance with their obligations by regulated entities. This Catalogue of risk indicators, therefore, seeks to help regulated entities fulfill their preventive obligations, an objective that Directive (EU) 2024/1640 pursues in Article 26(1)(a) when it urges Financial Intelligence Units (FIUs) to provide information *regarding "the types of transactions or activities that present a significant risk of money laundering, its underlying crimes, and terrorist financing".* This catalogue is an update of the one prepared in 2013 by the Commission for the Prevention of Money Laundering and Monetary Offenses in collaboration with the sector, which has been prompted by developments in operations and risks. Additionally, it includes a reference to high-risk operations in the case of lotteries, as well as high-risk activities generally carried out on online gambling platforms.

---

[1] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatfguidanceontherisk-basedapproachforcasinos.html

[2] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Vulnerabilities%20of%20Casinos%20and%20Gaming%20Sector.pdf.coredownload.pdf

[3] https://www.egba.eu/uploads/2023/03/230306-EGBA-Guidelines-on-AML-for-Online-Gambling-FINAL.pdf

[4] eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0344

This catalogue has been divided into two sections. The first section, “General Indicators,” includes indicators that, in principle, can be detected by any type of regulated entity. The second section, titled “Specific Indicators,” highlights others that refer to specific activities carried out only by certain types of regulated entities.

The indicators shown in the list are only a selection of the many indicators that can be found in money laundering, its various types of predicate offenses, and terrorist financing. An effort has been made to select those that are most evident and general. For indicators related to more specific typologies, the regulated entity may consult various publications by organizations and institutions that conduct studies on specific typologies, revealing the most frequent indicators. Likewise, it is recommended that the regulated entity add to the suggested list other indicators derived from cases it analyzes on its own and assesses as linked to terrorist financing, money laundering, and their underlying criminal activities.

Finally, the development of this catalogue has been accompanied by the preparation of a Report on the Most Commonly Used Criminal Typologies Today, classified according to the main underlying crime to which they are typically linked. The purpose of this document is to facilitate the work of regulated entities, insofar as a better understanding of the ways in which threats manifest in this area (drug trafficking, organized crime, corruption, etc.) can help improve the systems implemented by regulated entities to prevent and detect ML/TF transactions.

GENERAL RISK INDICATORS

In the process of performing due diligence

In the interaction between the regulated entity and its customer regarding due diligence, certain factors may arise that, while not preventing the completion of due diligence, are relevant in the context of detecting money laundering or terrorist financing. These include the following:

- In general, the customer's reluctance to provide information to the regulated entity during the course of the due diligence process.
- The customer's use of general terms such as "savings," "work," or similar expressions to inform the regulated entity about the source of their assets, in an attempt to avoid providing specific information about the nature of their employment, professional, or business activities.
- The cancellation of a transaction, or the modification of any of its characteristics (such as the amount), when the regulated entity requests that the customer provide additional documentation or information.
- The behavior of customers who demonstrate a high level of knowledge of AML/CFT regulations and an unusual interest in the procedures implemented by the regulated entity to ensure compliance.
- A request by the customer to the obligated entity not to comply with any of its due diligence obligations or with the proper recording of transactions, typically linked, either explicitly or implicitly, to whether or not new transactions will be carried out or to the continuation of the business relationship.
- The customer's demand for unusually high levels of confidentiality or discretion.
- Providing addresses as a primary residence that do not correspond to residential homes or premises for exclusive use, such as business centers, hotels, etc., when this is inconsistent with the regulated entity's knowledge of the customer, or with the number, amount, or profile of their transactions.

- A discrepancy between the country of residence declared by the customer to the obligated entity and the country of the address the customer provides for mailing correspondence, the country of the contact telephone number provided, or the country of the domain of their email account or website.
- Customers whose behaviour indicates adherence to radical extremist ideologies or who exhibit violent tendencies.
- Customers whose tax identification number (NIF) has been revoked at the time of conducting transactions or establishing business relationships, including those who are beneficial owners or directors of companies.

In remote transactions

By conducting remote transactions without direct contact with the regulated entity, it is possible to conceal the fact that those carrying out the transactions are not the individuals who have formally contracted with the regulated entity. Concealing the identity of the true person responsible for or the beneficial owner of the transactions is very common in ML/TF processes. The following are some indicators:

- Customers who systematically avoid conducting in-person transactions and instead carry out remotely transactions that are typically conducted in person.
- Access to the regulated entity's online services through the use of VPN services, proxy servers, or other mechanisms that conceal or hinder the geolocation of transactions.
- Frequent changes in IP addresses or devices when the same customer accesses the regulated entity's online services, without a justifiable reason.
- Attempts to open accounts or purchase products from IP addresses or devices previously used by customers other than those who intend to appear as the holders of the new account or the new product to be purchased, and without any apparent relationship between those former customers and the new customer.
- Attempts to purchase products remotely using the identity information of a customer already known to the regulated entity, when contact information is provided that does not match the information the regulated entity has on file for the known customer, or when there are other reasons to suspect that the customer's identity is being impersonated.

- Repeated access to the regulated entity's online services by the same customer from the same IP address, whose geolocation does not correspond to the location the customer has reported as their usual residence.
- Access to the regulated entity's online services by the same customer within a short period of time from several different connections that, based on their geolocation, are so far apart that it is not possible to travel from one to the other in the time elapsed between the connections.

Relocation of Transactions

As a result of economic globalization, international transactions are becoming increasingly common. However, on occasion, the international component is sought out deliberately, in an artificial manner, to distribute the elements of a single transaction across different jurisdictions and thus prevent the authorities of a single country from having a comprehensive understanding of the transaction. Such practices are common in AML/CFT processes. The following are some indicators:

- The execution of transactions that indicate or suggest the possibility that the regulated entity's customer has assets abroad, when this is inconsistent with the regulated entity's knowledge of the customer.
- The purchase of products in Spain by foreign individuals or legal entities, when there are no logical reasons for such purchases in our country.
- The operation of accounts domiciled in Spain (usually in branches located near the border with Spain or Portugal) that are limited to the mass receipt of transfers or other types of inflows originating in the other country, with the funds subsequently being disposed of through cash withdrawals or transfers to the same or another country.

Acting on behalf of a third party

Individuals involved in money laundering, its underlying crimes, and/or terrorist financing naturally seek to conceal their identity. To do so, they may use other individuals as frontmen who, acting on their instructions, interact with the regulated entities and formally appear as the account holders for the transactions.

The following are some indicators that may suggest the regulated entity's client is acting on behalf of another person:

- Cases in which a person acts, de facto or de jure, on behalf of the customer, when, based on the prevailing circumstances and the conduct of both parties, the regulated entity understands that decisions regarding the transactions or the business relationship are made by the representative, not the principal.
- Cases in which a person, whether a known client or a professional, acts as an introducer of a new client to the regulated entity, and it is the introducer who negotiates the new client's position vis-à-vis the regulated entity.
- A contract entered into by a new customer who provides the same address, telephone number, or email address as a previous customer, with whom they apparently have no relationship, and who carries out similar transactions.
- Cases in which it is observed that, in practice, there is a succession of one client by another, such that when the first terminates a business relationship, a new client—who formally appears to be independent of the previous one—establishes a new business relationship in which the same type of transactions are recorded.
- The actions of several clients acting as a group, such that each of them carries out a transaction with characteristics similar to those of the others, especially if it is observed that a third party, or one of them, is giving instructions to the others.
- Cases of remote onboarding where it appears that the new client is being assisted by a third party, for example, during the remote identification process via videoconference.
- The existence of several clients with no apparent relationship to one another who provide the same address, phone number, or email address, or who conduct online transactions via the same IP address.
- Changes to a client's contact information (phone number, email address) shortly after the account is opened or just before the client begins to execute trades.

Splitting of transactions

In many AML/CFT processes, a high volume of transactions can be suspicious. Furthermore, exceeding certain thresholds may require the regulated entity to implement enhanced due diligence measures or report information to the authorities. For this reason, transactions are very often split into several smaller ones, typically in the names of different individuals, so that each one is less conspicuous and does not trigger action by the regulated entity. The following are some indicators that a transaction has been split into several:

- The execution by a single customer, or by several acting in a coordinated manner, of multiple transactions of the same type, with the same origin and destination, consecutively, or within a short period of time, when, had the transaction been carried out in a single transaction for its total amount, the customer would have been required to provide additional information or documentation to the obligated entity.
- The purchase by the same person of many products, whether they are used simultaneously (the products are active at the same time) or successively (when one is canceled, another is purchased), carrying out a similar transaction.
- Cases in which a total payment is split into several payments, theoretically to benefit the payer, yet the time intervals between each payment are so short that they offer no practical advantage.

Place and time of transactions

Some indicators that take into account the place and time at which transactions are carried out are:

- Contracting a service or conducting a transaction in person at a location far from the customer's usual residence, when alternatives exist that would avoid the trip and there are no justifiable reasons for it.
- A customer repeatedly and systematically conducting transactions during peak hours at the regulated entity's premises, when it appears that this is an attempt to hinder the regulated entity's ability to perform due diligence or record the transactions.

- A customer's request that the transaction be completed within an unusually short timeframe, without a reasonable explanation for expediting the transaction, when it appears that this is an attempt to hinder the regulated entity's performance of due diligence.

Employees and Agents

Criminal organizations engaged in money laundering, their underlying criminal activities, and/or terrorist financing have significant financial resources and may bribe employees and agents of regulated entities to fail to apply adequate due diligence, fail to properly record transactions, or fail to report to the authorities. The following are some indicators that an employee or agent may have been corrupted:

- An employee's unjustified refusal to be promoted, take vacation, or make other changes that would result in losing direct contact with their clients.
- An employee displaying a standard of living higher than would be expected given their income, without a justifiable reason.
- An employee or agent experiencing a sudden, unexplained increase in the number of clients, the number or amount of their transactions, or the profile of those transactions.
- The concentration of transactions by an employee's or agent's clients on dates or at times that are normally periods of low public activity, without a justifiable reason.
- The agent's reluctance to comply with the regulated entity's AML/CFT measures, claiming that the measures established by other regulated entities for which they also act as an agent are more lenient.

Possible connection to criminal activities involving ML/TF

On occasion, the link between the customer or their transactions and criminal activities may be inferred by the regulated entity from its relationship with the authorities or may even be in the public domain. Some indicators are noted below:

- Transactions by customers regarding whom requests or inquiries for information are received from national authorities, in the context of an investigation into criminal activities.

- Transactions involving customers who are directly or indirectly linked to other customers regarding whom national authorities have issued requests or inquiries for information as part of an investigation into criminal activities.
- Transactions by customers for whom there is public information linking them to criminal activities.
- Transactions by customers that follow the same pattern and involve the same counterparties as those of other customers whose transactions were analyzed and found to be potentially linked to money laundering, underlying criminal activities, and/or terrorist financing.
- Customers subject to international sanctions, and persons associated with them.

RISK INDICATORS IN SPECIFIC ACTIVITIES

Gambling transactions in general.

- Clients who frequently engage in gambling transactions (banker and player, and/or betting) where low-risk bets are possible, or in card games (poker) where collusion among players is possible.

Online gambling transactions.

- Customers who use the same IP address and employ multiple identities or accounts to gamble.
- Customers who request changes to their previously provided information after registering on online gaming platforms, which may indicate the sale of the gaming account to another person.
- Customers who engage in activity at unusual times, dates, and periods, inconsistent with the professional or business activity declared to the regulated entity.
- When a customer, contrary to all logic, uses multiple different payment cards or accounts to deposit or withdraw funds from their gaming account.
- When several customers, with no apparent relationship to one another, nevertheless use the same card or bank account.
- When a customer systematically funds their gaming account using a specific payment method and withdraws the account balance to a different payment method, especially when deposits are made via card and withdrawals are directed to a bank account.
- A customer who requests to withdraw funds from their gaming account to third-party bank accounts.

- Maintaining high balances in the gaming account without a corresponding flow of bets.
- Depositing funds into a gaming account and withdrawing them after a period of time without having placed any bets.
- Customers who appear to be acting in concert to offset losses and winnings.
- Sports bets involving large sums of money on events of little sporting significance.
- The player uses an anonymous payment method, such as prepaid cards or eWallet[5] payment methods.

Casino transactions

- Customers who purchase a large number of chips with cash and/or small-denomination bills, participate only minimally in the game, and subsequently request to cash out the chips.
- Customers who, individually or in concert, repeatedly buy and sell chips over time for amounts below or very close to the legally established thresholds, with the aim of preventing casinos from complying with identification or document retention obligations.
- Customers who attempt to conduct currency exchange transactions at the casino that do not correspond to their gaming activity.
- Customers who, in a concerted manner, appear to hand over chips to one or more customers, without exceeding the limits established in gaming regulations so as not to be considered high-volume or high-risk.
- Transactions where prizes are awarded in the form of redeemable bearer tickets.

[5] The use of electronic wallets (eWallets) allows users to easily transfer funds between bank accounts, debit cards, or credit cards. These methods are difficult to trace and can offer a certain level of anonymity.

Lottery Transactions

- A customer who comes to collect winning tickets with different serial numbers at intervals over time.



September 2024

www.tesoro.es

secretariaICMC@economia.gob.es

Paseo del Prado 6, 28014, Madrid