CATALOGUE OF **RISK** INDICATORS

2024

Securities 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.

Furthermore, 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 (hereinafter "Law 10/2010 of April 28") designates, in Article 2.1, the following as regulated entities: investment firms (Art. 2.1.c); as well as

management companies of collective investment undertakings and investment companies whose management is not entrusted to a management company (Art. 2.1.d); management companies of venture capital entities and venture capital companies whose management is not entrusted to a management company (Art. 2.1.f); and management companies of closed-end collective investment undertakings and venture capital undertakings and other closed-end collective investment undertakings whose management is not entrusted to a management company.

As indicated in the National Risk Assessment (NRA) approved by the Commission for the Prevention of Money Laundering in 2020 and updated in April 2024, although investment firms, management companies of collective investment undertakings, and investment companies not managed by a management company have specific characteristics and particularities in the services they provide, in general, they present **a high inherent risk** of being used for money laundering, due to the possibility of obtaining a financial return on the invested funds and the opportunities these types of entities offer criminals to conceal the origin of the funds and their beneficial ownership. While the residual risk must be assessed on a case-by-case basis, depending on the type of services provided and the mitigating measures applied, in general terms the residual risk should be classified as moderate/significant. This finding is consistent with the

conclusions of the Supranational Risk Analysis prepared by the European Commission in 2022[1], which assigns a **"high" residual risk level** to the securities sector.

The securities sector is one of the main channels through which individuals and legal entities can access the financial system, thereby creating opportunities for abuse by criminals. For this reason, the Financial Action Task Force (FATF) published the report *"Money Laundering and Terrorist Financing in the Securities Sector"* in 2009 (FATF, October 2009), which describes various methods through which criminals can exploit this sector for money laundering and terrorist financing.

Furthermore, the FATF has recognized that adopting a risk-based approach is essential for the proper implementation of international standards on the prevention of money laundering and terrorist financing (AML/CFT). In this regard, the adoption of the report *"Guidance for a Risk-Based Approach for the Securities Sector"* (FATF, October 2018) is noteworthy; it describes the various types of entities that may be involved in a specific transaction in the securities sector, as well as their business models. The report also

[1] "COMMISSION STAFF WORKING DOCUMENT Accompanying the document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities", disponible en: eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0344

identifies the characteristic features of transactions in the securities sector that may create opportunities for criminals, as well as the measures that can be taken to address these vulnerabilities.

Furthermore, it should be noted that the FATF has produced various reports addressing horizontal issues that are also relevant to the securities sector. Among these, the *following reports* are particularly noteworthy*: "Beneficial Ownership of Legal Persons"* (FATF, March 2023); *"Misuse of Citizenship and Residency by Investment Programs" (*FATF, November 2023); and *"Crowdfunding for Terrorism Financing"* (FATF, October 2023).

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 securities sector. [2]

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.

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

This Catalogue of risk indicators, therefore, seeks to assist regulated entities in fulfilling their preventive obligations, an objective that Directive (EU) 2024/1640 pursues in its 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.

This catalogue is 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," lists others that refer to specific activities carried out only by certain types of regulated entities.

The indicators listed here are only a selection of the many indicators that can be found in money laundering, its various types of underlying crimes, and/or 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 refer to 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, or 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 schemes today, classified according to the primary 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 due diligence process

In the interaction between the regulated entity and its customer regarding due diligence, elements 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 refusal to provide information to the regulated entity during 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 private residences 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 the customer has declared to the regulated entity and the country of the address the customer provides for receiving mail, the country of the contact phone number provided, or the country associated with the domain of the customer's email account or website.
- Customers whose behavior indicates adherence to radical extremist ideologies or who exhibit violent tendencies.
- Customers whose tax identification number 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 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 at branches in locations near the border with Spain or Portugal) that are limited to the mass receipt of transfers or other types of income originating in the other country, with the funds subsequently being disposed of through cash withdrawals or transfers to the same or another country.
- In general, transactions involving structures spanning multiple jurisdictions, without a justifiable reason.
- The use of corporate structures in which the beneficial owner, the directors, or the company are located in different jurisdictions, without a justifiable reason.
- The use of corporate structures in which different companies from different

jurisdictions own one another, without a justifiable reason.

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 regulated entities and formally appear as the parties to the transactions. Below are some indicators that may suggest the regulated entity's customer is acting on behalf of another person:

- Cases in which a person acts, de facto or de jure, on behalf of the customer, where the regulated entity determines, based on the circumstances and the conduct of both parties, that decisions regarding transactions or the business relationship are made by the representative, not the principal.
- Cases in which a person, whether a known customer or a professional, acts as an introducer of a new customer to the obliged entity, and it is the introducer who negotiates the new customer's position with the obliged entity.
- A contract signed 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.
- Successive contracting with several companies, sometimes represented by the same individuals, such that once the transaction or business relationship of one of them ceases, another takes its place and carries out the same type of operations as the previous company, even with the same counterparties.
- 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 account opening 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 connection 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 adopt enhanced due diligence measures or report information to the authorities. For this reason, transactions are very often split into smaller ones, usually 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 regulated 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.

Regarding individuals or legal entities and beneficial ownership

Individuals involved in money laundering schemes and their underlying crimes naturally seek to conceal their identity. One method of concealment is the use of individuals or legal entities in which corporate positions and beneficial ownership are formally held by front men. Below are some indicators related to practices that are more closely linked to money laundering, although it is more difficult to find such indicators in terrorist financing offenses:

- Individuals or legal entities that experience frequent changes in the identification of their beneficial owner.
- Individuals or legal entities that declare a change in beneficial ownership without corresponding changes in their management or representatives.
- When there is evidence of a transfer of ownership of the company, but its representatives wish to rely on a beneficial ownership declaration made prior to the transfer.
- Individuals or legal entities that, in commercial practice, appear to be represented by persons who are neither their legal representative nor their beneficial owner.
- Individuals or legal entities whose beneficial ownership declaration is inconsistent with the information and documentation collected by the

reporting entity.

- Appointment of directors who clearly lack the necessary competence or suitability to perform the duties of the position.
- Use of companies, or other types of legal entities or structures, incorporated in foreign countries whose legal system permits the use of nominee shareholders, or allows the identification of the partner in a private document, such that in practice it is impossible to verify beneficial ownership through documentation.
- A beneficial owner who regularly appears in the incorporation or creation of legal entities or structures that are immediately transferred to another person.
- Simultaneous incorporation or creation of several legal entities or structures involving the same natural or legal person when there is no economic rationale or when anomalous circumstances exist.

Place and time of transactions

Some indicators that take into account the place and time in 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 a 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 involved 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 prevent them from conducting proper due diligence, failing to properly record transactions, or failing 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 by customers directly or indirectly related to other customers regarding whom requests or inquiries for information have been received from national authorities in the context of criminal investigations.
- 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

In securities account transactions

- Accounts that experience an unexpected increase in the number of transactions, or in the amount of such transactions, or significant changes in the type of transactions recorded, without this being consistent with the regulated entity's knowledge of its customer.
- Accounts that remain inactive for a period of time and then suddenly begin to show intense activity, without any known cause to justify it.
- Accounts which, due to the nature of the transactions, connections, devices, or for any other reason, may be suspected of being continuations of other accounts previously closed by the regulated entity for ML/TF prevention purposes.
- Transfers of securities or shares or units of Collective Investment Institutions to or from high-risk jurisdictions or tax havens, without a clear economic justification.
- A customer who displays a constant and systematic disregard for returns. In particular, the following transactions may fall under this category:

- A client who purchases shares or units and, upon selling them, does not care that losses have occurred that, given their profile, are significant.
- The client expresses the intention that the investment result be a loss.
- The client makes investment decisions that deviate from the investment policy and are contrary to their usual practice.

– The client gives express instructions to carry out portfolio management transactions against a specific entity or against a specific asset. (A planned change of ownership may be hidden behind this operation.)

– Trades in illiquid listed securities at prices that significantly deviate from market prices (e.g., trades in shares of investment companies at prices that significantly differ from the legal terms under which the company is required to provide consideration).

Transactions involving cryptoassets

– Clients who purchase cryptoassets with *fiat* currency and then instruct that their value be transferred to self-custody wallets or to wallets managed by an unregulated service provider.

– Customers who receive funds from self-custodial wallets or wallets managed by an unregulated service provider and intend to exchange them

for *fiat* currency.

- Customers who receive or send funds from services that, acting as transaction *mixers* or otherwise, seek to obscure the traceability of transactions.
- Wallets that, within a short period of time, accumulate funds from a number of theoretically independent customers who, however, connect to the regulated entity's platform from the same IP address.
- Wallets that aggregate significant funds received from a multitude of small transactions suspected of being related to peer-to-peer (P2P) exchanges or similar activities.
- Customers who receive funds from wallets whose addresses appear in open sources linked to commercial activities inconsistent with the regulated entity's knowledge of the customer, or to illicit businesses advertised on the dark web.
- Transactions involving crypto-assets that contain messages referring to illicit activities or the purchase of goods such as drugs, weapons, information, etc.
- Customers who receive a high volume of cryptoassets in their wallets that is inconsistent with the information provided to the regulated entity or with their operational history.
- Customers who inform a regulated entity that the source of their assets, or

of the funds used in a transaction, are profits from investments in cryptoassets, when the information and documentation provided does not allow for the traceability of the transactions through which the investment was made to be identified or for the profits obtained to be verified.

Securities Transactions

- Changes to a customer's information, followed by changes in their trading instructions that may indicate a hidden change in the ultimate ownership or control of an account.
- Frequent changes in the accounts used by the same client, with the aim of hindering the tracking of their transactions.
- Submission of securities lending agreements or other transactions involving a change of ownership to jurisdictions that hinder or prevent the investment services firm from obtaining information on the successful completion of the transaction, when such submission is not justified.
- Instructions to dispose of the proceeds from the settlement of transactions in favor of third parties other than the account holder, without any apparent economic rationale.
- Fund transfers issued from a significant number of accounts and received

by an investment fund (or by several funds managed by the same manager) for the subscription of shares in the name of the same client.

- Transactions involving the design or request by the client for the design of OTC structures (custom-designed transactions between counterparties not traded on organized secondary markets), with or without the use of derivatives, where such use has no apparent lawful or economic purpose.
- Instructions for the settlement of transactions that deviate from normal, customary, or logical patterns from a market practices perspective (for example, the use of securities lending for settlement without the loan being repaid—whether or not collateral exists—when the characteristics of the client and their ordinary or reasonably expected operations do not provide a clear rationale for such a transaction).
- Participation in financial swap agreements on the OTC market, and subsequent settlement using funds of illicit origin.
- Purchases and sales of OTC securities where the means of payment used cannot be traced or where there is a lack of substantive information necessary for traceability.
- Transfers of securities to or from high-risk jurisdictions or tax havens, without a clear economic justification.



September 2024

www.tesoro.es

secretariaICMC@economia.gob.es

Paseo del Prado 6, 28014, Madrid