CATALOGUE OF **RISK** INDICATORS

2024

Payment institutions, electronic money institutions, currency exchange institutions, or money transfer or remittance service providers.

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 establishes the status of obligated entity in Article 2.1(h), (i), and (j) for payment institutions, electronic money institutions, currency exchange businesses, or entities engaged in money transfer or remittance activities.

Thus, as noted in the National Risk Assessment approved by the Commission for the Prevention of Money Laundering and Monetary Offenses in 2020 (updated in April 2024), the **inherent risk in the payment institution sector is very high** for various reasons, related to both endogenous and exogenous factors. Thus, payment institutions and their branches and agencies pose a higher risk than other regulated entities due to their ability to channel funds, making them an attractive system for transferring illicit funds. This is due, on the one hand, to the fragmentation of their operations, as a large number of customers carry out many small-value transactions, and, on the other hand, to the existence of a significant number of small-scale establishments that handle money transfers on an agency basis (each payment institution may have thousands of agents). All of this hinders the proper oversight of these establishments by the authorities and by the payment institutions themselves, which has facilitated the use of agents and small establishments for money laundering and terrorist financing activities by criminal networks. In the case of **electronic money institutions**, the National Risk Assessment also assigns a **very high inherent risk** common to the entire sector. These risks are higher for electronic money issued in other countries where controls on the holder's identity and transaction thresholds do not meet the requirements mandated at the national level.

However, with regard to the residual risk in both cases, the implementation of risk-based anti-money laundering and countering the financing of terrorism (AML/CFT) measures has led to increased monitoring and supervision of these transactions and the adoption of specific preventive measures by these entities, which have led to a significant mitigation of risks, although it is understood that a significant residual risk remains for both money laundering and terrorist financing.

As for the **currency exchange sector**, the National Risk Assessment assigns a **high inherent risk** to these transactions due to the very nature of the activity, both in the case of transactions related to **money laundering** and those related to **terrorist financing**. Thus, in the first case, the high risk is determined by its close relationship with the movement of cash and the resulting difficulties in identifying its origin, its traceability, anonymity, and ease of transport, among other factors. In the second case, the typical terrorist financing schemes used by jihadist threats often rely on cash due to the numerous advantages it offers. Subsequently, it is necessary to carry out a currency exchange transaction to convert the funds into internationally accepted currency. Furthermore, conversion operations are particularly attractive to terrorists on the move, as well as for obtaining financing for terrorist groups in third countries.

However, despite the sector's high risk, regulatory licensing and registration requirements, monitoring of its activities by the Bank of Spain, growing technological development, adherence to a strengthened customer due diligence regime, and the sector's institutions' high level of awareness regarding their ML/TF prevention obligations and supervision, the **residual risk level is progressively decreasing**.

For its part, the **money order sector** faces **high inherent risks**, particularly in activities linked to terrorist financing. However, the provision of the service by a public operator, the specific regulatory amendments approved for payment institutions—which are applicable to money orders to strengthen the prevention regime—the engagement by supervisory authorities, and the effectiveness of internal policies and procedures regarding ML/TF prevention, imply a substantial reduction in the sector's risk profile. This risk should be considered **low** for use in **money laundering** operations and for all money orders that originate from and are destined for the postal service provided by the State-owned company Correos y Telégrafos, S.A., S.M.E. (Correos), but it should be considered **moderate** regarding potential links to **terrorist financing** operations in money orders when the money

orders originate from and are transferred through other operators.

Thus, in 2016, the Financial Action Task Force (FATF) published guidelines for a risk-based approach to money remittance or transfer transactions[1]. Similarly, the European Banking Authority issued Guidelines on money laundering and terrorist financing risk factors in 2021[2].

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 specific risks associated with payment institutions, electronic money institutions, currency exchange businesses, and entities engaged in money transfer activities[3].

This Catalogue has been prepared by the Commission for the Prevention of Money Laundering and Monetary Offenses, in the exercise of its functions, in collaboration with industry associations, with the aim of assisting regulated entities in complying with their obligations. This Catalogue of risk indicators, therefore, aims to help regulated entities fulfil 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"*.

[1] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Rba-money-or-value-transfer.html

[2] EBA GL 2021 02 - consolidated (amended by EBA GL 2023 03)_ES.docx (europa.eu)

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

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 industry, prompted by changes in operational practices and risks. This catalogue also includes operations related to electronic money institutions that were not covered in the previous catalogue.

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,” highlights others that pertain 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 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, 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 offense 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 obligated 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 behaviour of customers who demonstrate a high level of knowledge of anti-money laundering (AML) and counter-terrorism financing (CTF) 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 (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 the contact information provided does not match the information the regulated entity has on file for that 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 (typically at branches located near the border with Spain or Portugal) that are limited to the bulk receipt of transfers or other types of inflows originating in the other country, with the

funds subsequently being made available 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 schemes, their 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, when, based on the circumstances and the actions of both parties, the regulated entity understands that decisions regarding the transactions or the business relationship are made by the representative, not the represented party.

- Cases in which a person, whether an existing customer or a professional, acts as an introducer of a new customer to the regulated entity, and it is the introducer who negotiates the new customer's position with the regulated entity.
- A contract entered into by a new customer who provides the same address, phone 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, one client is succeeded by another, such that when the first client 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, gives instructions to the others.
- Cases of remote onboarding where it appears that the new customer is being assisted by a third party, for example, during the remote identification process via videoconference.

- The existence of multiple customers with no apparent connection to one another who provide the same address, phone number, or email address, or who conduct online transactions using the same IP address.
- Changes to a customer's contact information (phone number, email address) shortly after the account is opened or just before the customer begins to conduct transactions.

Splitting of transactions

In many AML/CFT processes, the high volume of transactions can raise red flags. 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.

Regarding individuals or legal entities and beneficial ownership

Individuals involved in money laundering schemes and their underlying crimes naturally seek to conceal their identities. One method of concealment involves 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 these indicators are more difficult to identify in cases of terrorist financing:

- 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.
- The 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 systems permit the use of nominee shareholders or allow the identification of the shareholder in a private document, such that, in practice, it is impossible to verify beneficial ownership through documentary evidence.
- A beneficial owner who regularly appears in the incorporation or formation of legal entities or structures that are immediately transferred to another person.
- Simultaneous incorporation or creation of multiple 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 at which transactions are carried out include:

- 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 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 accept a promotion, 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 anti-money laundering measures, claiming that the measures established by other regulated entities for which they also act as an agent are more lenient.

Possible connection to ML/TF criminal activities

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 involving customers for whom there is public information linking them to criminal activities.
- Customer transactions that involve the same type of activity and 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.

- Clients subject to international sanctions, and persons associated with them.

RISK INDICATORS IN SPECIFIC ACTIVITIES

In cash transactions

- The execution of a cash payment when, due to the amount, the nature of the transaction, or other circumstances, the use of cash was not expected.
- Transactions involving the transfer of money to beneficiaries using cash, where it is detected that the transfers are made by different individuals or by the same individual in multiple installments, without a justifiable reason.
- The purchase of bearer payment instruments, such as non-registered prepaid cards or electronic money, in exchange for cash, especially when the instruments are not presented for redemption within a reasonable period of time.
- Cash deposits into non-registered products where, due to the splitting of the deposits, the identity of the person making them is unknown, or when such identification is hindered by the customer's avoidance of the regulated entity's branches.

- Cash withdrawals charged to balances generated through POS transactions, when the frequency and amounts suggest an operation involving cash delivery in exchange for a debit to the card account.
- Cash remittances in which counterfeit bills appear more frequently than usual.
- Fundraising operations involving funds from various sources (online platforms, PSCA, payment platforms, etc.) that are withdrawn in cash.

Regarding account operations

- 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 that channel funds received from a single payer to multiple payees, or that receive funds from multiple payers to a single payee, without this being consistent with the regulated entity's knowledge of its customer.
- Accounts which, due to the coincidence of the origin or destination of funds, the type of transaction, connections, devices, or for any other reason, may be suspected of being continuations of other accounts previously closed by the regulated entity for AML/CFT reasons.

- Accounts whose sole activity is the receipt of fund transfers from third parties, the amount of which is immediately disposed of through cash withdrawals, transfers abroad, or transfers to crypto-asset service providers.
- Accounts that show a pattern of receiving transfers from crypto-asset service providers, immediately followed by the withdrawal of funds in cash or the issuance of transfers to third parties.
- Accounts whose sole or nearly sole activity is the receipt of one or more fund transfers from third parties, the proceeds of which are immediately withdrawn via cash withdrawals, international transfers, or transfers to cryptoasset service providers.
- Accounts of Publicly Exposed Persons that receive transfers from third parties without a commercial rationale.
- Customer accounts that, for no apparent commercial reason, are used to purchase airline tickets for third parties bound for countries at risk of terrorism or linked to human trafficking.
- Accounts with deposits indicating that the account may be used for fundraising for alleged charitable purposes, especially if it is a personal account and/or if the funds are immediately withdrawn in cash.
- Accounts used, without just cause, to purchase weapons or dual-use items that could be used in terrorist attacks or in a war context (ammunition, explosive materials, or their precursors, military military such as clothing, optical optical or electronic equipment, satellite phones, etc.).

In payment transactions

- Fund transfers where the beneficiary indicated by the payer does not match the account holder of the receiving account.
- Fund transfers in which the payment descriptions indicated by the payer are inconsistent with the declared activity or with the operational history of the recipient account holder.
- Fund transfers in which the payment descriptions refer to illegal or prohibited activities, or to payments for goods such as drugs, weapons, information, etc.
- Transactions in online accounts at unusual times.

In money transfer transactions

- A customer who makes two or more transfers using different types of identification documents (for example, a passport for one and a residence card for another), if the combined amount requires the regulated entity to apply enhanced due diligence measures.
- A customer who appears nervous, hesitant, or needs to consult others to provide the required information about the beneficiary and destination of the transfer they are attempting to initiate.
- A customer who provides clearly fictitious names as recipients of the transfer (for example, names of artists, athletes, or famous people).

- A customer who orders a shipment for a significantly higher amount and to a different country and beneficiary than those of other shipments previously ordered by the same customer.
- Transactions ordered by multiple customers from the same location or nearby locations within a short period of time that share the same characteristics (amount, destination country, destination city, etc.)
- Transactions in which a recipient, particularly in or near conflict zones, receives funds from multiple individuals—including from various countries—within a short period of time, known as a "time window," during which the recipient accumulates multiple transfers; this pattern typically repeats cyclically with various recipients.
- Sending funds to a new identity following the cancellation of a previous transfer intended for a different recipient.
- A customer whose transactions are continuously blocked by the payment institution due to existing issues with the recipient of the transfers.
- An agent whose number of new customers, relative to the number of regular customers, is higher than usual, especially if the transactions of new customers exhibit characteristics different from those of regular customers.
- An agent who conducts an unusually high number of transactions, or transactions involving unusually high amounts, or both, especially if they are concentrated in the same destination country.
- Agent conducting a substantial volume of transactions destined for the same city or geographic area, without a justifiable reason.

- An agent with a high number of senders whose nationality or country of origin differs from the destination country of the payment transactions.
- Agents who do not properly retain documentation evidencing the execution of transactions, or who do not correctly record all data in the transaction log.
- An agent whose name, or that of their relatives or employees, appears as the originator of money transfer transactions to different countries or beneficiaries.
- An agent who processes a substantial volume of transactions in which the senders and recipients are interrelated without a valid reason, either because different senders are sending money to the same recipient(s), or because different recipients are receiving money from the same sender(s).
- Entities whose customers place a large number of money transfer orders for amounts slightly below the thresholds established by regulation for the application of enhanced due diligence measures.

Electronic money transactions

- Distribution through intermediaries that are not obligated entities, when the electronic money issuer:
    - uses the intermediary to fulfil some of the AML/CFT obligations of the electronic money issuer; and
    - has not verified that the intermediary has adequate AML/CFT systems and controls in place.

Cryptoasset transactions

- Customers who purchase cryptoassets with fiat currency and then instruct that the value be transferred to self-custodial 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 aggregate funds from a number of theoretically independent customers within a short period of time and that, nevertheless, connect to the regulated entity's platform from the same IP address.
- Wallets that hold significant amounts of funds received from a large number 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 do not allow for the traceability of the transactions through which the investment was made to be identified or the profits obtained to be verified.



September 2024

www.tesoro.es

secretariaICMC@economia.gob.es

Paseo del Prado 6, 28014, Madrid