CATALOGUE OF **RISK** INDICATORS

2024

Valuables: jewelry, gemstones, precious metals, art, and antiques.

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 activity, may assist the entity in developing its own catalogue 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, establishes that natural or legal persons who professionally trade in jewelry, precious stones, or precious metals, as well as in works of art or antiques, are considered 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, jewelry, precious metals, and gemstones carry an inherent risk of being used in money laundering and terrorist financing operations, as they can concentrate significant economic value in a very small size, making them easy to transport. Additionally, they do not lose value over time but

rather appreciate, and their price often depends on the buyer. In short, gold and other precious metals and stones are attractive for concealing illegal funds or making payments for criminal activities. For organized crime groups, which are one of the main threats in this sector, the use of precious stones and metals can serve as a highly useful system for paying for illicit transactions, offering advantages such as ease of storage, value retention, the untraceability of their origin, or the possibility of successive deliveries, among others.

The risks in the sector are primarily associated with the method of payment, the customer profile, and the type of transaction. The frequent use of cash, installment payments, or the endorsement of other transferable means of payment facilitate anonymity and make it difficult to identify the final buyer. Additionally, some jewelry and works of art may be small in size, meaning they can be hidden or transported from one place to another without being detected, which facilitates the cross-border movement of illicit proceeds.

In light of these inherent risks, there are a number of factors and mitigating measures that significantly reduce the level of residual risk. Among these, the following stand out: increased awareness among sector entities regarding AML/CFT prevention —which has improved substantially in recent years— and the enforcement of prevention obligations. Consequently, the residual risk level is considered moderate for money laundering and moderate/low for terrorist financing.

The National Risk Assessment approved by the Commission for the Prevention of Money Laundering in 2020, updated in April 2024, notes that the inherent risk in the sale of art and antiques stems from a number of reasons: the use of intermediaries that facilitate anonymity and the concealment of the true owner's and the customer's identity; the difficulty in tracing these items and the funds involved, which can hinder the investigation of potential crimes given how quickly they can change hands. It is also a market that is difficult to control, in which informal channels for the sale of goods exist outside the ordinary trade of professionals. As this is a market where the identification and valuation of objects—some of which have high economic value—attracts organized crime groups, both nationally and globally, it allows for the concealment of illicit funds through the acquisition of these goods, investment in them, and the preservation of their value for

subsequent sale and recovery of funds.

However, in the face of these inherent risks, there are a number of factors and measures that mitigate the resulting risk, due to the high degree of specialization and a recognized code of ethics, which enables these professionals to identify clients and transactions most likely to be linked to illicit activities. This is compounded by the fact that the average transaction amounts are not high, and the sector's economic volume is not particularly significant in our country. As a result of these measures, the residual risk is lower and is considered moderate for both money laundering and terrorist financing.

In this context, the Financial Action Task Force (FATF) has expressly included professionals engaged in commercial activities involving precious stones and metals as regulated entities for the purposes of preventing money laundering and terrorist financing and has issued risk reports on the matter. Specifically, in FATF Report[1], *"Money Laundering and Terrorist Financing Risks and Vulnerabilities Associated with Gold"*, dated July 2015, it is noted that it is the characteristics of gold that make it an attractive and vulnerable asset for exploitation by criminal organizations seeking to legitimize their assets.

Gold has intrinsic value, is easy to exchange worldwide, and can be traded anonymously, just like precious metals and gemstones. In some countries, existing gold market regulations may make its use attractive to organized crime groups since a large portion of transactions can be conducted in cash and, in many cases, there is no record of the proper identification of the seller or buyer of the gold. The FATF report also notes that gold is easy to melt down and convert into common forms, allowing it to be concealed from border authorities and avoiding their intervention.

[1] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/ML-TF-risks-vulnerabilities-associated-with-gold.pdf.coredownload.pdf

In the case of the trade in art, antiques, and other cultural objects, and although the FATF does not consider them to be regulated entities, it constitutes a multi-billion-euro industry that attracts organized crime groups seeking to launder proceeds of crime and finance their activities, due to the high prices these items can command and the privacy and discretion surrounding the identities of buyers and sellers, as noted in FATF Report[2], *"Money Laundering and Terrorist Financing in the Art and Antiques Market"*, dated February 2023. This risk justifies their inclusion as regulated entities under Law 10/2010 of April 28, as well as in the recently adopted European regulations. The status of regulated entities entails a legal duty to comply with a series of obligations regarding the prevention of money laundering and terrorist financing, as detailed in Law 10/2010 of April 28 and in the implementing regulations.

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 for 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."*

[2] Spanish-ML-TF-Art-Antiquities-Market.pdf.coredownload.pdf (fatf-gafi.org)

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, and was prompted by changes 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"* highlights others that pertain 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, the 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/or their underlying criminal activities.

Finally, the preparation of this Catalogue has been accompanied by the preparation of a Report on the Criminal Typologies Most Commonly Used 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 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 reluctance 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 anti-money laundering (AML) and countering the financing of terrorism (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 using IP addresses or devices previously used by customers other than those who claim to be the holders of the new account or the new product to be purchased, and where there is no apparent relationship between those previous 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 that 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, 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 represented party.
- 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.
- 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 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 customers acting in concert, of multiple transactions of the same type, with the same origin and destination, either consecutively or within a short period of time, when, had the total amount been transacted in a single transaction, the customer would have been required to provide additional information or documentation to the regulated entity.

- The purchase by a single person of many products, whether they are used simultaneously (the products are active at the same time) or successively (when one is cancelled, 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, its underlying crimes, and/or terrorist financing 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 frontmen. The following are some indicators related to this:

- 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 declaration of beneficial ownership 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 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 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 criminal activities related to 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 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.
- Customers subject to international sanctions, and persons associated with them.

RISK INDICATORS IN SPECIFIC ACTIVITIES

Art, jewelry, and antiques

- Customers who purchase high-value items, or in quantities exceeding the norm, and do not demonstrate knowledge or experience in the sector.
- Transactions in which customers show little interest in the characteristics of the item, do not negotiate the price or terms, and request that the transaction be completed within a very short timeframe.
- Parties who request or offer, in their sales transactions, the return or repurchase of the merchandise, especially when cash or funds from sensitive territories were used in the prior purchase, despite any penalties that may have been established.
- Any transaction with a representative in which the identity of the owner, beneficial owner, or relevant person remains concealed, contrary to the normal procedure for the type of business in question.
- Transactions in which significant payments are made in cash, by bearer checks, by endorsement of other negotiable instruments, or by other anonymous means, without a logical explanation.

- Deferral of payment to a date very close to the time of purchase, especially if no guarantee is provided to secure it, without a logical explanation.
- Transactions in which there are discrepancies between the address listed in the details of the person presenting themselves as the buyer and the address where the goods are to be delivered, without any justification for this.
- Auctions in which a prior agreement is detected between the seller and the person who, ultimately and regardless of price increases, will proceed to purchase the auctioned item.
- Transactions in which there is suspicion that the buyer of precious metal intended for smelting is not using it for industrial purposes.



September 2024

www.tesoro.es

secretarialCMC@economia.gob.es

Paseo del Prado 6, 28014, Madrid