

**GOOD PRACTICES ON THE PREVENTION OF MONEY
LAUNDERING AND TERRORIST FINANCING IN THE
NOTARIAL SECTOR**

2018

INDEX

Contents

1. INTRODUCTION.....	3
2. PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING OBLIGATIONS	5
a. DUE DILIGENCE OBLIGATIONS	5
b. OBLIGATION TO RETAIN DOCUMENTATION OR KEEP RECORDS.....	6
c. OBLIGATION TO IDENTIFY POLITICALLY EXPOSED PERSONS	6
d. IMPLEMENTATION OF INTERNAL CONTROL MEASURES.....	7
e. OBLIGATION TO REPORT SUSPICIOUS TRANSACTIONS	7
3. GENERAL PRINCIPLES OF THE ANTI MONEY LAUNDERING AND TERRORIST FINANCING MODEL	8
a. RISK APPROACH	8
b. AWARENESS OF THE NOTARY AND ALL EMPLOYEES.....	8
c. UNIVERSALITY	9
d. ADJUSTMENT TO THE ACTIVITY CARRIED OUT.....	9
e. PILLARS OF PREVENTION	9
f. PRACTICAL AND UPDATED DOCUMENT	10
4. GOOD PRACTICES FOR COMPLIANCE WITH ANTI MONEY LAUNDERING AND TERRORIST FINANCING OBLIGATIONS.....	11
1. PRIOR RISK ANALYSIS.....	11
a. Risk inherent to the customer	11
b. Geographic/country risk	14
c. Risk of service offered.....	15
2. DEVELOPMENT AND APPLICATION OF DUE DILIGENCE MEASURES	17
a. Normal or standard due diligence measures.....	18
b. Enhanced due diligence measures	20
c. Simplified Due Diligence Measures	21
3. RECORDS KEEPING OR MAINTENANCE OF RECORDS	21
4. IMPLEMENTATION OF INTERNAL CONTROL MEASURES.....	22
5. REPORTING SUSPICIOUS TRANSACTIONS.....	23

1. INTRODUCTION

In 1989, at the initiative of the G-7, an intergovernmental body known as the Financial Action Task Force (FATF) was created to coordinate efforts to prevent money laundering in both the international financial system and the national financial systems of the member entities.

The FATF's main objective is to develop and promote policies to combat money laundering and terrorist financing. It is the body that sets and oversees international standards for regulations against money laundering and terrorist financing.

The FATF first issued a comprehensive plan, known as the Forty Recommendations, to combat money laundering intended to present the basic framework for anti-money laundering (AML) efforts, implementing measures in 2002 to combat Terrorist Financing (CTF) and to be of universal application.

In its 2003 review of the Recommendations, the FATF sought the support of so-called 'guardians' to combat money laundering and terrorist financing. Thus, it included, among others, certain designated non-financial businesses and professions (DNFBPs) such as lawyers, notaries, trust and company service providers (TCSPs), real estate agents, accountants and auditors who assist with transactions involving the movement of money in national and international financial systems.

Countries have adopted different approaches for regulating notaries as obliged subjects to the compliance of these Recommendations in the notarial sector.

In addition, among the Member Countries, there are some systems for the prevention of money laundering and the financing of terrorism in the notarial sector, where the assessment of the sector's risk and the development of the internal control policies and procedures for AML/CFT are the responsibility of the self-regulatory bodies, which guarantees homogeneity and uniformity in the requirements for the application of these policies throughout the notarial sector.

In order to facilitate notaries' compliance with the obligations established by the FATF and recognized at the national level by most countries of the world through specific regulations on Anti Money Laundering and Terrorist Financing (AML/CTF), in particular in cases where the Self-Regulatory Bodies have not been involved in it, the International Union of Notaries has prepared this AML/CTF best practice document.

This is not a single and comprehensive model, since the incorporation of the FATF Recommendations in the legislation regarding AML/CTF of the different member countries may differ in some respects, but rather a guide that must in all cases be adapted to the reality of each notary, in accordance with their practice and the requirements of their local regulations.

Likewise, the degree of exposure to risk, the different notarial functions, the different possibilities for the introduction of funds into the legal system in accordance with the practice carried out, in short, the risk of notaries regarding anti money laundering and terrorist financing may be very different. The greater the risk, the higher the level of

awareness among notaries and the stronger the control mechanisms and prevention measures they should have in order to implement effective prevention.

This document consists of a brief explanation of the obligations to prevent money laundering and terrorist financing to which, in accordance with the FATF Recommendations, notaries are or should be subject, without prejudice to any additional obligations which may be established by the local regulations of AML/CFT; a section of general principles and a final section specifying good practices for compliance with prevention obligations.

2. PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING OBLIGATIONS

FATF Recommendation 22 states that notaries shall be subject to the obligations of **(a) customer due diligence, (b) record keeping, (c) identification of Politically Exposed Persons, (d) implementation of internal control measures and (e) reporting of suspicious transactions** when they prepare to carry out transactions or are conducting transactions for a client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

These obligations should be implemented applying a risk-based approach. This means that notaries must identify, assess and understand their money laundering and terrorist financing risks and develop their policies and procedures to assess risks, and apply resources to ensure that they are mitigated effectively.

By adopting a risk-based approach, notaries should be able to ensure that measures aimed at preventing or mitigating money laundering and terrorist financing correspond to the risks identified, allowing them to make decisions on how to allocate their own resources in the most effective way.

As stated in the introduction, these are the minimum obligations required by the FATF, without prejudice to any additional obligations that may be established by local AML/CFT regulations. For this reason, each notary must check the possible additional AML/CFT obligations established by their country.

a. DUE DILIGENCE OBLIGATIONS

‘Customer due diligence (CDD)’ involves identifying and getting to know all natural or legal persons intending to establish business relationships or conducting any transactions, and it is not possible to maintain business relationships or carry out transactions with natural or legal persons that have not been properly identified.

The CDD measures to be implemented are the following:

- (a) **Identifying the Customer¹** and **verifying the identity** of the customer using reliable, independent source documents, data or information.
- (b) **Identifying the beneficial owner** (beneficial owner) and taking reasonable measures to verify the identity of the beneficial owner, so that the notary is convinced that they know who the beneficial owner is. For legal persons and

¹ The customer must be understood as any party involved in the transaction, not only those paying the notary fees.

other legal arrangements, this includes notaries understanding the ownership and control structure of the customer.

- (c) Understanding, and as appropriate, obtaining **information on the purpose** and intended nature of the business relationship.
- (d) Conducting **ongoing due diligence** on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the notary's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds. This obligation must be understood in the case of longer-term business relationships and the notary's involvement in an occasional transaction is not necessary.

b. OBLIGATION TO RETAIN DOCUMENTATION OR KEEP RECORDS

As required by FATF Recommendation 11, notaries must keep for at least five years²: all records obtained for compliance with the due diligence obligation (e.g. copies of records of official identification documents like passports, identity cards, driving licences or similar documents), including the results of any preliminary analyses undertaken (e.g. Inquiries to establish the background and purpose of complex, unusually large transactions) after the date of the transaction.

They must also keep all necessary records on the transactions carried out with the customer, both locally and internationally, in order to make them available to the authorities.

Due diligence information and transaction records should be made available to domestic competent authorities upon appropriate authorisation.

c. OBLIGATION TO IDENTIFY POLITICALLY EXPOSED PERSONS

This obligation means that notaries, in addition to ensuring that they identify whether the customer or beneficial owner is a Politically Exposed Person (PEP), must apply **enhanced due diligence measures**.

This implies, first of all, that appropriate risk management systems must be in place to determine whether the customer or the final beneficiary (beneficial owner) is a politically exposed person.

Likewise, in the event that the customer or the final beneficiary should satisfy this condition, notaries must be familiar with this circumstance at the time of execution of the transaction with the customer and must adopt reasonable measures to establish the origin of the assets and the origin of the funds which the customer intends to use in the transaction.

² This period may vary by country. As already indicated, the time limit provided for in each country's internal AML/TF regulations should be consulted.

Requirements for all types of PEPs should also apply to family members or close associates of said PEPs.

d. IMPLEMENTATION OF INTERNAL CONTROL MEASURES

As indicated at the beginning, another of the obligations established by the FATF for notaries is the implementation of internal control measures.

These internal control programmes mean that notaries must:

- **Establish AML/CFT policies and procedures** that will be applicable at their office, including adequate screening procedures to ensure high standards when hiring employees.
- Develop and maintain an **ongoing internal and external employee training programme**; and
- Establish an **internal verification procedure** to self-assess the operation of the system.

These internal control measures will depend on the money laundering and terrorist financing risk identified in the required risk self-assessment and the scale of the professional activity.

e. OBLIGATION TO REPORT SUSPICIOUS TRANSACTIONS

This obligation implies that if the notary suspects or has reasonable grounds to suspect that the funds are the result of criminal activity, or are related to terrorist financing, they must report it promptly to the Competent Authority determined by local regulations (the Financial Intelligence Unit (FIU) or similar).

The obligation to report suspicious transactions also includes a prohibition on tipping-off the customer or third parties that such a report or related information is being provided to the FIU or the Self-Regulatory Body.

Furthermore, the AML/CFT Law of each country must expressly provide that prosecution authorities are not allowed to disclose the names of the reporter to the suspects and for the protection of **notaries against criminal and civil liability** for violation of any restriction on the disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, by the 'good faith' report produced, even if they do not know precisely what the underlying criminal activity is, and regardless of whether the illegal activity actually occurred.

3. GENERAL PRINCIPLES OF THE ANTI MONEY LAUNDERING AND TERRORIST FINANCING MODEL

In accordance with the requirements derived from international standards, the effective implementation of an internal AML/CFT system must be governed by general principles, including the following:

a. RISK APPROACH

The prevention procedures must be developed in accordance with the ML/TF risk inherent in the activity and the regulated subject's way of operating.

This means that when drafting, developing and implementing their respective policies, procedures and manuals on prevention, notaries should take into account and adapt due diligence measures with clients following a **risk-based approach**, that is, depending on the risk of ML/TF inherent in the nature of its activity, its relative size, the customs and practices of the business, its type of clientele, whether or not cash is handled, the geographical area in which it operates, etc.

The aim is that, through the proper application by notaries of this approach, a more efficient use of the available resources is achieved and there is a reduction in the burdens incurred by participating in the national prevention system.

To this end, in order to achieve a correct assessment and understanding of the risk regarding ML/TF, notaries must draw up a document or report, which is mainly practical and adapted to the business they explain, describe and assess their exposure to ML/TF risk in relation to their activity.

This report will identify the risk elements which in the field of ML/TF could affect the business carried out by the notary. The extent and depth of the document or report will depend on the notary's level of risk in relation to their activity. In any case, the minimum contents of the report are detailed in point a) of section 3 of this document. This risk assessment on money laundering and terrorist financing report must be available to the competent Authorities, as it will allow to explain the suitability of the AML/CFT policies and procedures adopted by the notary.

b. AWARENESS OF THE NOTARY AND ALL EMPLOYEES

The notary is responsible and is legally obliged to comply with the AML/CFT measures. They must therefore be aware of the risks of ML/TF and ensure that the necessary measures are taken to mitigate these risks at their office.

The notary is responsible for the AML/CFT policies and measures implemented to manage ML/TF risk. This means that they should be aware of the ML/TF risks they are exposed to and ensure that all employees are aware of those risks and take the necessary measures to effectively mitigate them.

Therefore, the notary must actively participate in the prevention system in place and provide internal and external training in this regard to all employees at the notary's office.

They should also be involved in the AML/CFT work, so policies, procedures and manuals developed, produced and implemented in relation to AML/CFT, regardless of size or turnover, must be approved by them.

c. UNIVERSALITY

There are countries in which prevention procedures in the notarial sector must be applied following a principle of universality, in other words, any customer with whom business relationships are established, or any transaction in which action is taken, either more regularly or on an occasional basis, must be subject to the application of such prevention on a prior basis, and in accordance with an analysis of the risks raised by each of them in terms of prevention.

In other words, no customer or transaction may be excluded from the scope of prevention, including specifically those transactions which do not originate or are executed through the usual business channels (e.g. corporate or one-off operations, property sales, credit portfolio sales, etc.).

Irrespective of the criterion and scope established by each country, in accordance with the terms of FATF, prevention procedures must in all cases be applied where the notary intervenes in or authorises transactions or carries out transactions for their customers regarding the activities included in Recommendation 22, as set out in Section 2, and those which, in addition, the legislator may have previously included in each country, and on the basis of an analysis of the risks posed by each of them in terms of prevention.

d. ADJUSTMENT TO THE ACTIVITY CARRIED OUT

Naturally, the activity carried out by notaries differs from that of other regulated subjects obliged to comply with the regulations regarding AML/CFT. This means that the procedures, manuals and software used must be fully adapted to the specific activity carried out by the notary and to the different activities performed, as well as the services they offer, to the different markets in which they operate, and to the customers with whom they interact.

e. PILLARS OF PREVENTION

In any case, the pillars on which the procedures on AML/CFT should be based for notaries, taking into account the application of the risk approach referred to above, are those that allow correct **customer identification**, the **identification of the final beneficiary** of the transactions carried out, **knowledge of the source of the funds** employed by customers, as well as the **consistency of transactions** carried out by the customer with the knowledge of the regulated subject and of their business and risk profile.

To this end, and prior to the establishment of the business relationship, all documentation and information relevant to the specific case must be requested and

obtained in accordance with the risk presented.

f. PRACTICAL AND UPDATED DOCUMENT

Prevention measures must not be a reiteration of the current regulations, they must describe the procedures effectively implemented in a practical way. The prevention manual must be adapted to changes in service delivery and procedures.

Meanwhile, prevention measures that notaries may draw up, develop and implement must comply with the operational reality of the procedures at any given time, and must not simply be a mere reiteration or a copy of the generic obligations set out in the regulations in force. Policies, procedures and manuals that do not conform to the operational reality of the notary cannot be considered adequate, nor those which simply list their prevention obligations without specifying the way in which each of these obligations will be implemented in practice and effectively.

In short, the aim is to make the AML/CFT a practical and easy-to-use document, not a purely formal document, allowing its effective application and easy adaptation to the activities carried out by the notary and to any changes which may occur in such procedures and activities.

4. GOOD PRACTICES FOR COMPLIANCE WITH ANTI MONEY LAUNDERING AND TERRORIST FINANCING OBLIGATIONS

1. PRIOR RISK ANALYSIS

The risk or degree of exposure of regulated subjects regarding attempts at money laundering or terrorist financing is very different. Risk is determined by quantitative and qualitative aspects, both closely linked to the type of activity carried out by each regulated subject.

Consequently, the structures, internal control procedures, tools and resources to be employed for prevention by notaries must be adapted to this different risk.

The pillars of ML/TF prevention, namely the due diligence measures (identification of the formal and beneficial owner, and knowledge of their activity, which will include an understanding of the origin of the funds with which the customer intends to operate with the regulated subject), are covered by the application of the risk approach.

To this end, and in order to adopt appropriate measures to identify and assess their money laundering and terrorist financing risks, in accordance with the requirements of the FATF Recommendations, notaries must carry out an analysis of the risk of money laundering and terrorist financing to which they are exposed.

In determining or analysing this risk, 3 categories or risk factors are identified internationally:

- a. Risk inherent to the customer
- b. Geographic/country risk
- c. Risk of service rendered

The relative weight to be assigned to each risk category when assessing the overall risk of money laundering and terrorist financing will vary depending on the notary due to the size, sophistication, location and nature and scope of the services offered.

Based on their individual practices and judgements, notaries will need to independently assess the weight given to each risk factor.

a. Risk inherent to the customer

A critical component in the development and implementation of a global framework risk is to determine the potential for money laundering or terrorist financing risk posed by a customer. Customers range from natural persons, associations, limited liability companies, companies with multiple members or members of multinational corporations. Given this spectrum of customers, the notary must determine whether a particular customer poses a greater risk and, if so, the level of that risk and whether the application of any mitigating factors influence that assessment.

If a customer belongs to one of these categories, a set of risk variables that can mitigate or exacerbate the risk must be implemented and the notary must carry out an

assessment to determine the required level of due diligence.

Examples of categories of customers whose activities may indicate increased risk include:

- Politically exposed persons. Politically exposed persons (PEPs) are individuals who are or have been entrusted with prominent public functions domestically or by a foreign country, such as Heads of State or Government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations and officials of important political party officials. This also includes persons who are or have been entrusted with a prominent function by an international organisation, who are members of senior management, i.e. directors, deputy directors and members of the boards or equivalent functions.

The definition of a PEP is not intended to cover middle ranking or more junior individuals in the foregoing categories.

If a notary carries out a transaction for a customer who is a PEP or owned by the PEP, they are required to perform a higher and more demanding form of due diligence, known as 'enhanced due diligence'. The extent and nature of the enhanced due diligence will depend on the relevant factors, such as the PEP's country of origin, the type of service required by the PEP and the scrutiny to which the PEP is subject in their country of origin.

To identify whether the customer is a PEP, the notary may ask the customer, and there are also companies dedicated to providing lists of PEPs through the contracting of licenses.

- Customers who carry out their business relationship or request services under unusual or unconventional circumstances (as assessed from all the circumstances of the representation).
- Customers where the structure or nature of the entity or relationship makes it difficult to identify in a timely manner the true final beneficiary or those exercising control, such as:
 - Unexplained use of legal entities or legal agreements, named shares or bearer shares.
 - Unexplained use of informal agreements, such as relatives or close associates acting as nominee shareholders or directors.
 - Unusual complexity in control or ownership structures without a clear explanation.
- Customer legal person that operates a substantial part of their business or has significant subsidiaries in countries that may have a greater geographical risk.
- Cash-intensive business customers³ (and/or cash equivalents), including:
 - Money service businesses (e.g. remittance operators, currency exchange

³ When customers that are cash-intensive business are themselves subject to and regulated by a full range of AML/TF requirements consistent with the FATF Recommendations, this can mitigate risks.

offices, bureaux de change, exchange centres, money senders, money exchange offices, money transfer agents and banknote traders or other companies offering money transfer services).

- Operators, brokers and other service providers using virtual currencies.
- Casinos, betting shops and other gambling-related organisations and activities.
- Companies that, although not normally cash-intensive, appear to have substantial amounts of cash.
- Charities and other non-profit organisations (NPOs) that are not subject to supervision or surveillance (especially those operating on a cross-border basis) by designated competent authorities or self-regulatory bodies.
- Customers using financial intermediaries, financial institutions or legal professionals who are not subject to adequate AML/ATF laws and measures and who are not adequately supervised by competent authorities or self-regulatory bodies.
- Customers who appear to be acting according to another person's instructions without revealing this fact, and who denies to disclose the information when required.
- Customers who avoid face-to-face meetings or provide intermittent instructions without legitimate reasons and who are otherwise elusive or very difficult to reach.
- Customers requesting that transactions be completed in tight or accelerated time frames, making it difficult or impossible for the notary to carry out an appropriate risk assessment.
- Customers who have no address, or multiple addresses without legitimate reasons.
- Customers whose profile (e.g. age, training, income or activity) is not consistent with the transaction they intend to carry out.
- Customers who change their settlement or execution instructions without a proper explanation.
- The use of persons and legal structures without an apparent legal or lawful legitimate, commercial, economic or other reason.
- Customers who change their means of payment for a transaction at the last moment and without justification (or a suspicious justification), or when there is a lack of information or transparency regarding the transaction.

- Customers who offer to pay extra fees for services that would not normally warrant said amount.
- ‘Shell’ companies, companies owned through nominal shareholders, and control through nominee and corporate directors.
- Multiple related customers requesting the services of the same notary for related matters without a legitimate reason.

b. Geographic/country risk

Bearing in mind that there is no universally accepted definition by international organisations that stipulates whether a particular country or geographical area represents a greater risk, the country risk, together with other risk factors, provides useful information on possible money laundering and terrorist financing risks.

Geographical money laundering and terrorist financing risks may arise in a variety of circumstances, including the customer’s place of nationality, the place of residence, the location of the transaction or source of funding.

Factors generally considered to include a country in a higher risk category are:

- Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations (UN). Moreover, in some circumstances, countries subject to sanctions or measures issued by bodies similar to the UN, although they may not be universally recognised, may be taken into account due to the situation of the issuer of the sanctions and the nature of the measures.
- Countries identified by credible sources⁴ as generally lacking appropriate laws, regulations and other AML/CFT measures.
- Countries identified by credible sources as providing funding or support to terrorist organisations.
- Countries identified by credible sources as having significant levels of corruption or other criminal activity. Specially concerned jurisdictions may include ‘extraterritorial jurisdictions’ and those with high political instability or low levels of AML/CFT compliance or insufficient rule of law enforcement.
- Countries that allow the use of nominee shareholders and bearer shares,

⁴ ‘Credible sources’ refers to information that is produced by known bodies that are generally considered to be of a good standing and that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, among others, supranational or international bodies such as the International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-governmental organisations. The information provided by these credible sources does not have the effect of laws or regulations and should not be viewed as an automatic assessment that a certain circumstance poses a greater risk.

allowing the final beneficiary to be hidden.

- For national customers, the geographical risk that may exist in specific areas could also be considered, such as proximity to the border, free trade zones or areas where there is a large population of immigrants from high-risk countries.

c. Risk of service offered

A general risk assessment should also include assessing the potential risks presented by the services offered by the notary, taking into account that in most cases notaries provide a broad and diverse range of services.

The context of the services offered is always fundamental to a risk-based approach. Any of the above factors alone cannot constitute a high-risk circumstance, but the factors should be considered jointly.

High-risk circumstances can only be determined by careful assessment of a number of factors which, jointly and after taking into account any mitigating circumstances, would justify further risk assessment. When determining the risks associated with the provision of services related to specific activities, factors such as the following should be taken into account:

- Services where notaries, acting as financial intermediaries, handle the receipt and transmission of funds through accounts they actually control in a commercial transaction process.
- Services that unduly hide beneficial ownership from the competent authorities, or that have the effect of wrongfully hiding the beneficiary ownership without any clear legitimate purpose.

Services that rely heavily on new technologies that reduce the level of human oversight or due diligence on material that could reveal patterns of illicit or suspicious behaviour. The risk could be mitigated depending on the technology used by the notary

- Transfer of immovable property between parties over a period of time that is unusually short for similar transactions for no apparent legal, taxation, business, economic or other legitimate reason.
- Payments received from unaffiliated or unknown third parties and cash payments where this method of payment is not typical.
- Transactions related to inheritance law where the deceased was known to the notary as a person who had been convicted of economic crimes.
- The source of funds and the source of wealth: the source of funds is the activity that generates the funds for a customer (such as salary, business income or payments from a trust), while the source of wealth describes the activities that have generated the total net worth of a customer (for example, ownership of a

business, inheritance or investments). While these may be the same for some customers, they may be partially or totally different for other customers. For example, a PEP who receives a modest official salary, but has a substantial bank account balance, with no apparent commercial interest or inheritance, may raise suspicions of bribery, corruption, or abuse of position.

- Situations in which it is difficult to identify the beneficiaries of the trusts; this could include a discretionary trust that gives the custodian discretion to appoint the beneficiary within a class of beneficiaries and distribute the assets held in trust accordingly, and when establishing a trust for the purpose of managing shares in a company that may make it more difficult to determine the beneficiaries of the assets managed by the trust.
- Use of virtual currencies and other anonymous means of payment and wealth transfer.
- Transactions using unusual means of payment, such as precious metals or where there is an apparent desire to hide the payment.
- Deferment of a payment to a date far after the payment would normally be carried out, without guarantees securing the payment and/or without explanation.
- Unexplained establishment of unusual terms or clauses in credit agreements. For example, unusually short or long repayment periods, interest rates significantly higher or lower than those on the market, single payment refund on the due date, or unexplained repeated cancellations of promissory notes or mortgages substantially prior to the originally agreed maturity date.
- Contributions to societies or transfers of assets that are inherently difficult to assess (such as jewellery, precious stones, art objects or antiques, virtual currencies), without an explanation.
- Subsequent unexplained capital contributions or other short-term contributions to the same company.
- Liquidating business acquisitions without any apparent legal or legitimate, commercial, economic or other reason.
- Powers of attorney given under unusual conditions (e.g. where they are granted irrevocably or in relation to specific assets) and the reasons given for these conditions are not clear or are illogical.
- Transactions involving closely connected persons without a clear business purpose or where the transaction does not appear to be under the arm's length principle.
- Transactions with guarantees located or originating in at-risk jurisdictions.

- Transactions in which, in spite of the notary's warning, more taxes are paid than are legally due for their conception.
- Transactions in which, although the nationality or residence of customers is not an at-risk jurisdiction, funds originated or destined to such jurisdictions are used.

Due attention should be paid to large differences in practices, size, scale and experience among notaries. As a result, these factors must be considered when creating a reasonable risk-based approach and resources that can reasonably be allocated to implement and manage it.

For example, a notary working alone would not be expected to devote an equivalent level of resources as a large notary office; rather, the only notary would be expected to develop appropriate systems and controls and a risk-based approach proportionate to the scope and nature of the practice of the professional and its customers.

That said, notaries in many jurisdictions and practices are obliged to carry out an assessment of the general risks of their practice, and of all new customers and current customers involved in specific, one-off transactions. The emphasis must be on a risk-based approach.

The risk assessment will be subject to periodic review and, in any event, where there is a significant change that could influence the notary's risk profile, such as the provision of new services or the use of new technology, with appropriate measures in place to manage and mitigate the risks identified in the analysis.

2. DEVELOPMENT AND APPLICATION OF DUE DILIGENCE MEASURES

As we have indicated in Section 2, irrespective of the criterion and scope established by each country, in accordance with the terms of FATF, prevention procedures must in all cases be applied where the notary intervenes or authorises transactions or carries out transactions for their customers regarding the activities included in Recommendation 22, as set out in Section 2, and those which, in addition, the legislator may have previously included in each country, and on the basis of an analysis of the risks posed by each of them in terms of prevention.

The pillars of the money laundering and terrorist financing prevention system are based on the proper identification of the customer, the identification of the final beneficiary of the transactions carried out, the knowledge of the source of funds used by customers, the consistency of the transactions carried out by the customer with the knowledge the notary has regarding the customer and the business and risk profile related to them.

The key starting point for implementing a risk-based approach is to conduct an overall customer risk assessment.

The procedures described in this Section are designed to complement, not substitute, that system. The complexity of this system will vary depending on the notary's practice

profile.

As previously seen, when carrying out an overall assessment of the customer's risk, the notary should consider taking into account appropriate risk variables (and any mitigating factors) before deciding to accept the customer. The notary's risk assessment, which is carried out on an individualised basis for each customer, will dictate the general approach to customer identification and verification requirements.

The notary will determine which due diligence requirements are appropriate for each customer based on the general risk assessment. These due diligence requirements may include the following:

a. Normal or standard due diligence measures

A standard level of due diligence generally applies to all customers. The standard level of due diligence includes the following elements:

- **Identifying the customer and verifying that customer's identity using reliable, independent source documents**, data or information. As we have seen in Section 2, the notary **must keep** for the period required by their internal regulations, a **copy of all documents obtained for compliance with the duty of due diligence** (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents).

- **Basic identification:**

- **For natural persons**, basic identification and verification of the customer's identity involves obtaining (and recording) personal data such as full name, national identity number, address, date and place of birth, place of residence, by applying for the official identification document such as passports, identity cards, driver's licenses or other document issued by a government authority **bearing a photograph of the holder**.

To prevent the fraudulent use of documentation, there are applications or software on the market that can be used to scan documents and identify whether they are fake.

- **For legal persons**, the type of information that would normally be needed to perform this identification would be:
 - **Name, legal form and proof of existence** – verification could be obtained, for example, through a certificate of incorporation, a certificate of good standing, and a partnership agreement, a deed of trust or other documentation from a reliable independent source proving the name, form and current existence of the customer.
 - **The powers that regulate and bind the legal person or**

arrangement (e.g., memorandum and articles of association of a company), as well as the names of the relevant persons having a senior management position in the legal person or arrangement (e.g., senior management directors in a company, trustee(s) of a trust).

- **The address of the registered office**, and, if different, a principal place of business.
 - **Identification and verification of the identity of the person(s) acting on behalf of the customer and obtaining the powers of attorney.**
- **Checking, before initiating the relationship, the relevant lists of financial sanctions** (terrorist financing and proliferation) to confirm that the customer or final beneficiary is not listed or included on any of them. These lists are publicly available on the United Nations website and there are also companies dedicated to providing such lists through licensing.
- Identify the beneficial owners and take reasonable measures to verify identity of such persons, so that the notary is reasonably satisfied with knowing who the beneficial owner is, by means of the following information:
 - For legal persons:
 - The identity of the natural persons, (if any, as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control over the legal person or arrangement through ownership) who ultimately have a controlling ownership interest in a legal person; and
 - to the extent that there is a doubt under (i.i) as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or whether the natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person or arrangement through other means.

Whenever possible, , a good practice is to request the public deed or documentation of the ownership structure or control structure of the legal person for the purposes of verifying the information provided by the customer about the final beneficiary or access to Beneficial Owners databases or registers, if they exist in the country.

- For legal arrangements:
 - Trusts - the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or classes of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership)

- Other types of legal arrangements – the identity of persons in equivalent or similar positions.

The FATF authorises the relevant identification data to be obtained from a public register, the customer or other reliable sources, and the notary must therefore ensure in the manner established and authorised by their local regulations.

The general rule is that customers must be subject to the full range of due diligence measures, including the requirement to identify the final beneficiary. The purpose of identifying the final beneficiary is to determine the natural persons who exercise effective influence or control over a customer, whether by ownership, voting rights or otherwise. Notaries should take this objective into account when identifying the final beneficiary. They may use a risk-based approach to determine the extent to which they should verify the identity of the final beneficiary, depending on the type of customer, the business relationship and the transaction, and other appropriate factors.

- Obtain information on the purpose of the transaction and the economic activity carried out by the customer.

Some countries also require verification of the activity declared by the customer in cases of higher risk. To this end, as an alternative to requesting said documents from the customer, in some countries it is possible to access the Tax or Labour Administration databases.

- Scrutinise the transaction(s) carried out to ensure that the transactions carried out are consistent with the knowledge of the notary about the customer, the business and risk profile, including, where necessary, the source of funds.

b. Enhanced due diligence measures

The application of enhanced due diligence measures is required for customers who may be expressly indicated in local regulations, as well as for those customers determined by the notary, applying their risk-based approach as being of greater risk.

These enhanced measures imply that, in particular, the degree and nature of the business relationship monitoring should be increased in order to determine whether the required transaction or service appears unusual or suspicious.

Examples of enhanced due diligence measures that can be applied to higher risk customers include:

- Obtaining additional information and documentation on the customer (e.g. volume of assets, information available in public databases, internet, etc.) and final beneficiary.
- Obtaining additional information on the nature of the commercial relationship.
- Obtaining information on the source of the customer's funds or assets.

- Verification of the final beneficiary's identity by requesting identity documents.

c. Simplified Due Diligence Measures 5

The application of normal or standard due diligence measures may be reduced after considering appropriate risk variables and in recognised lower risk scenarios, such as those recognised by international standards:

- Listed companies (and their majority-owned subsidiaries). Although it should not be assumed that all publicly traded companies will qualify for simplified due diligence, for example, appropriate levels of market reporting will be considered as a factor to be taken into account, as well as geographical risk factors.
- Financial institutions (domestic or foreign) subject to an AML/CFT regime consistent with the FATF Recommendations.
- Government authorities and public sector entities (other than sanctioned and high-risk countries).

Reduced due diligence may include simply obtaining information and documentation on the customer's identity, identifying and verifying the identity of the person acting on behalf of the customer and their powers of attorney, sufficient information to prove that the customer meets objective characteristics for the application of these measures, among others.

Simplified due diligence measures may not be applied where there is a suspicion of money laundering or terrorist financing or where they are applied in specific higher risk scenarios.

Bearing in mind that the vast majority of countries expressly state in local regulations the categories of customers which may be subject to simplified due diligence measures and the measures to be applied in these cases, the notary is advised to ensure the measures applicable in their country.

In those jurisdictions which allow reliance on third parties, the notaries have the possibility of conducting the due diligence measures relying on information provided by third parties allowed by the Law, as well as other notaries, while the ultimate responsibility for observance of all AML/CTF compliance duties must ultimately rest with the notary even when he relies on third parties.

3. RECORDS KEEPING OR MAINTENANCE OF RECORDS

Among the obligations detailed above, the notary must keep for the period established by their local regulations the documentation formalising compliance with the due diligence obligations established by this.

⁵ In most countries, local regulations expressly stipulate customer categories that may be subject to simplified due diligence.

In particular, notaries must keep the following documentation for use in any investigation or analysis of possible money laundering or terrorist financing cases by the competent authorities:

- A copy of required documents under due diligence measures.
- Original or copy with evidential value of the documents or records that adequately credit the operations and the participants involved in them.

To this end, as a good practice, a large majority of the local regulations of the countries regarding AML/CFT indicate that the documentation obtained in application of due diligence measures must be stored on optical, magnetic or electronic media guaranteeing their integrity, the correct reading of the data, the inability to manipulate them and their proper conservation and location.

As a result, the notary must ensure the requirements and format for record-keeping derived from their local regulations.

In any case, in the absence of specific requirements or formats, the filing system of the regulated subjects must ensure adequate management and availability of the documentation, both for internal control purposes and for the purposes of timely and formal attention to the requirements of the authorities.

4. IMPLEMENTATION OF INTERNAL CONTROL MEASURES

As indicated in Section 2, notaries must implement internal control measures which entail:

- establishing AML/CFT policies and procedures that will be applicable at their office, including adequate screening procedures to ensure high standards when hiring employees;
- developing and maintaining an ongoing internal and external employee training programme; and
- establishing an internal verification procedure to self-assess the operation of the system.

These internal control measures, which will depend on the risk of money laundering and terrorist financing identified in the risk self-assessment and the size and scope of the notary organisation, should include:

- Having appropriate risk management systems to determine whether a customer, prospective customer or final beneficiary is a PEP or a designated person and included on any of the specific financial sanctions lists (financing and proliferation of terrorism).
- Provide a greater focus on notary transactions (e.g. services, customers and geographic locations) that are more vulnerable to abuse by money launderers.

- Provide a periodic review of the management processes and risk assessment, taking into account the environment in which the notary operates and the activity in their market.
- Implement risk-based customer due diligence policies, procedures and processes.
- Designate personnel at an appropriate level who are responsible for managing AML/CFT compliance.
- Provide programme continuity despite changes in employee administration, composition or structure.
- Focus on complying with all regulatory records or other requirements, as well as measures enacted to comply with AML/CFT and provide timely updates in response to regulatory changes.
- Provide adequate controls for higher risk customers and services as needed.
- Incorporate compliance with AML/CFT measures into relevant personnel job descriptions and performance assessments.
- Provide appropriate training for all personnel involved.
- Consider the application of new technologies for conducting the due diligence measures, as long as the notary intervenes in the process and remains responsible for the adoption of the final decision on the risk assessment.

As we have stated in the introduction, among the member countries, there are some systems for the prevention of money laundering and terrorist financing in the notarial sector, where the assessment of the sector's risk and the development of the policies and procedures for AML/CFT and the training of notaries and employees of notaries' offices are the responsibility of the self-regulatory bodies, which guarantees homogeneity and uniformity in the requirements for the application of these policies throughout the notarial sector.

This practice has demonstrated its effectiveness in the level of compliance with AML/CFT obligations in the sector, and therefore the high involvement of the Self-Regulatory Bodies in this regard is recommended.

It is likewise recommended that the Self-Regulatory Bodies also be involved in the development of training plans for the notarial sector, either through the provision of online or on-site courses and establish consultation systems for notaries where each notary can resolve potential doubts regarding compliance with the obligations of the AML/CFT.

5. REPORTING SUSPICIOUS TRANSACTIONS

As we have stated, this obligation implies that if the notary suspects or has reasonable grounds to suspect that the funds are the result of criminal activity, or are related to

terrorist financing, they must report it promptly to the Competent Authority determined by local regulations (the Financial Intelligence Unit (FIU) or similar).

This reporting obligation extends to both transactions carried out and transactions attempted by customers.

In addition to this, the obligation to report suspicious transactions also includes a prohibition on tipping-off the customer or third parties that such a report or related information is being provided to the FIU or the Self-Regulatory Body.

Countries have taken different approaches to fulfil this obligation in the notarial sector. Some countries adopted the model of direct report by the notary to the competent Authorities, but by virtue of what is permitted by the FATF Recommendations provided there are appropriate forms of cooperation between these organisations and the competent Authorities, in some countries, the AML/CFT system in place establishes that the report is made to the Self-Regulatory Bodies (Councils or Notary Chambers) and said Body is responsible for forwarding it to the competent Authority, but without applying any filters and only with the analysis carried out by the notary.

Likewise, in other countries there are models in which, by virtue of the identification of certain risk indicators in a given transaction, the notary must notify this transaction to a Specific Analysis Unit established within the Self-Regulatory Body, comprising professionals with experience in AML/CFT, in order for said Unit to carry out an analysis of the possible link between it and money laundering or terrorist financing, and decide on the need to notify the competent Authority.

Therefore, the system in place at the local level for compliance with the system must be verified.

In any case, notaries should be aware of the requirements in their jurisdictions regarding the obligation of non-disclosure and/or any obligation to refrain from transactions suspected of involving criminal activity. These obligations, if implemented, can lead to serious sanctions if not properly enforced.

When a legal or regulatory requirement requires the reporting of transactions when there is a suspicion, a report must always be produced and therefore a risk-based approach to reporting suspicious transactions under these circumstances is not applied.

Reports of suspicious transactions are not part of the risk assessment, but rather reflect a response mechanism, either to the Self-Regulatory Body or the Competent Authority, once a suspicion of money laundering or terrorist financing has been identified.