LIGHT
Illuminating Dark Corners

Co-funded by the Justice Program
(2014-2020) of the European Union

Good Practices of AML/CFT for notaries and lawyers

GRANT AGREEMENT NUMBER 101007890

Content

Acronyms

AML/CFT	Anti-Money Laundering/Counter Financing of Terrorism
ATM	Automated Teller Machine
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
ICO	Initial Coin Offering
ILP	Independent Legal Professional
NFT	Non-Fungible Tokens
RBA	Risk-Based Approach
SDD	Simplified Due Diligence
SRB	Self-Regulated Body
STR	Suspicious Transaction Report
VA	Virtual Assets
VASP	Virtual Assets Service Provider

Introduction

The project on "Legal competency preventing AML/CFT: Illuminating Dark Corners" (hereinafter the "LIGHT Project" or the "Project") aims to increase the legal competency and then ensure the effectiveness of AML/CFT policy regarding lawyers and notaries in Belgium, Bulgaria, Italy and Spain.

The Project stems from the 2019 Commission Staff Working Document (SWD 650/2019) which complained on the involvement of legal professions in ML/FT schemes in the creation of opaque structures.

In its second supranational risk assessment, the Commission identified 47 products and services that are potentially vulnerable to money laundering and terrorist financing risks, compared to 40 in 2017.

Among the "additional supporting measures", the report recommends again *"Training for professionals engaged in activities covered by "professional secrecy", providing guidance and practical insights to help them recognize possible money laundering or terrorist financing operations and how to proceed in such cases".*

Hence, LIGHT Project encompasses a series of phases that start with the assessment of the implementation of EU law on AML/CFT in the different national contexts (carried out by different national focus groups); continues with the development of a policy statement on the role of legal professions for an effective implementation of AML/CFT; prepares training activities (materials preparation, training of trainers, student selection); implements online training and face-to-face seminars; collects professional good practices from the attendees of such seminars; and, sets a European conference to present the alliance between notaries and lawyers on the EU AML/CFT effectiveness, as well as a link with enforcement (Europol) to liaise on the most effective preventive measures legal professionals can assist with.

The four transnational face to face seminars covered all subjects identified by the training need analysis. The idea was to exploit the cross-border nature of ML/FT to share a common vision and modus operandi in EU AML/CFT, and to provide a list of good practices as follows:

1. "Reducing red tape", as discussed during the seminar that took place in Rome (Italy), in March 2022.
2. "Mitigating vulnerabilities", as set forth during the seminar conducted in Brussels (Belgium), in April 2022.
3. "Questing red flags", as dealt with at the seminar held in Sofia (Bulgaria), in May 2022.
4. "New crypto crimes", as collected at the seminar hosted in Madrid (Spain), in June 2022.

This document refers to the detailed best practices collected during the training activities encompassed during the Project. This is not a single and comprehensive model, since the incorporation of the EU Directives and 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 legal professional, in accordance with their practice and the requirements of their local regulations.

1. Reducing red tape

The content of the first Seminar, held in Rome, was the **"EU AML/CFT architecture and role of legal professions"**, with the aim to gather best practices in **"Reducing red tape"**. The best practices collected during the seminar are set forth in the following subsections:

During the Seminar, the authorities present noted the need for legal professionals as guardians of legality in countering anti-money laundering phenomena. While believing that automated reports based on the most sophisticated artificial intelligence tools are important, it emerged that the presence of highly qualified professionals who intercept transactions at their genesis and who know how to detect the presence of dangerous indexes as soon as possible is essential.

Thus, there was a common feeling and wish for constant training in AML/CFT, and how the ideal professional regarding AML/CFT, is that of an independent, authoritative person who has a loyal collaborative role with public authorities. In this, the notary figure was recognized as the most effective, especially in countries where the Self-Regulatory Bodies (SRBs) are involved in the practical compliance with the obligations of the AML/CFT measures in the sector, through the centralization of the analysis of suspicious transactions, the development of guidelines and common rules, training plans and the provision of consultation systems for professionals where they can resolve potential doubts regarding compliance those obligations.

It also emerged how, in order to avoid the risk of superfluous documentation production by professionals, due to (i) the need to demonstrate compliance with AML/CFT procedures that for the Supervisory Authorities derive from primary and secondary legislation - and (ii) the increase in unimportant reports, it is appropriate that the sanctions imposed are felt to be fair and balanced and differentiated - as among other things provided for in the legislation - according to the organization and structure of the reporter.

In this regard, during the seminar the experiences of the operators were compared, and some elements emerged that can be indicated as indicators of risky operations, in the presence of which it is necessary to report the operation to the public authorities. In order to collect them in a single body, which can be an integral part of a virtuous practice, reference is made to the anomaly index, in the presence of which the operator must always deepen the analysis of the case and if necessary, report the transaction to the competent authorities.

Below are the main features of the Italian regulation on anomaly index and revised according to the results of the Seminar:

- Purchase of goods at a very high price compared to the economic-asset profile of the customer or group to which they belong in the absence of reasonable reasons or specific needs.

- Purchase or sale of goods at a price that is clearly disproportionate to their market value in the absence of reasonable reasons or specific needs.
- Purchase of goods carried out with the acquisition of shares of companies based in countries with anti-money laundering regime not equivalent to that of the European Community countries in the absence of reasonable reasons or specific needs.
- Request, in the absence of reasonable reasons, for professional services which, even via corporate transactions, have the purpose or effect of concealing or hindering the identification of the beneficial owner of the activity or to conceal the origin or destination of the financial resources involved.
- Frequent and unjustified changes in the ownership or name of companies and businesses.
- Establishment and / or use of trusts, in the event that a specific legislation of countries with anti-money laundering regime not equivalent to that of the European Community countries is applied.
- Establishment and / or use of artificially complex and articulated group structures, also in relation to the distribution of shareholdings and the relocation abroad of one or more companies.
- Establishment and / or employment of investee companies by incapable persons, except in the case of family-run businesses, or the conferment of positions of responsibility in companies or entities to persons clearly lacking the necessary skills.
- Issue of powers of attorney to manage, administer and / or sell assets, especially if immediately following the purchase of the asset or in favor of persons apparently not connected to the delegator.
- Contributions or contributions of capital in companies or other entities through assets in kind for amounts clearly disproportionate to those of the market.
- Proposal to settle payments by means of instruments that are completely inconsistent with the current practice of the requested operation, in the absence of reasonable reasons linked to the type of activity carried out, to any corporate group to which the customer belongs or to particular conditions adequately documented.
- Recourse for significant amounts to cash, bearer passbooks or other bearer securities, as well as foreign currency and gold. c. Frequent and unjustified use of non-registered electronic money, especially if for overall significant amounts.
- Proposal to settle payments in a manner that raises doubts as to whether it intends to resort to techniques for dividing the economic value of the transaction, in the absence of reasonable reasons linked to the activity carried out or to particular conditions adequately documented.
- Request, in the absence of reasonable reasons, to modify the payment methods already agreed, especially if payment instruments are proposed that are not appropriate to the common practice of the arranged operation.

- Payment of operations or services by means of payment coming, for various reasons, from third parties unrelated to the contractual relationship and not attributable to the customer's group, or in any case not connected with the customer, in the absence of reasonable reasons.
- Request for professional services or for the completion of operations having an object or purpose that is not compatible with the economic-patrimonial profile or with the client's activity or with the economic patrimonial profile, or with the activity of any corporate group to which the same belongs.
- Consultancy for the organization of financial transactions that are inconsistent with the underlying commercial activity.
- Services requested by non-profit organizations for purposes that are not compatible with those declared or in any case proper to the entity.
- Request for advice for the execution of structured finance transactions on international markets for needs related to a commercial activity with foreign countries of evidently limited size.
- Purchase of availability for various reasons of goods, including luxury goods, of high value, against a small amount of assets, including group assets.
- Frequent operations for the acquisition of shareholdings or other rights on companies or companies, not justified by the economic - patrimonial profile or by the activity of the customer or of any corporate group to which the same belongs or for other reasonable reasons.
- Financial transactions of considerable amount, especially if requested by recently established companies, not justified by the purpose of the company, by the customer's business or by any corporate group to which the same belongs or by other reasonable reasons.
- Purchase of equity investments in companies in ways that are inconsistent with the economic-patrimonial profile or with the activity carried out by the customer or by any corporate group to which the same belongs or for other reasonable reasons.
- Request for professional services in an unusual and clearly unjustified manner with respect to the normal performance of the profession or activity.
- Request for professional service to a professional located in a location far from the area of residence or from the actual place of business of the client in the absence of plausible reasons such as, but not limited to, the foreign citizenship of the client or his group to which he belongs or specialization specification of the professional in relation to the professional service requested.
- Recourse to post office boxes or postal addresses other than the tax or professional domicile, or other forms of convenient domiciliation.
- Frequent release by natural persons of proxies or powers of attorney in order to avoid direct contact with the professional.
- Frequent request for transactions on behalf of a third party in the absence of reasonable reasons related to the type of activity carried out or to the

relationship between the parties or to particular conditions adequately documented.

- Request for professional services or for carrying out operations with an illogical configuration, especially if economically and financially disadvantageous for the customer or in an excessively complex manner with respect to the stated purpose.
- Request, in the absence of reasonable reasons, to change the conditions and methods of carrying out the professional service, especially if the requested changes involve additional charges for the customer.
- The customer provides information that is clearly inaccurate or incomplete or false regarding: his own identity and that of any beneficial owner; the purpose and nature of the requested service; the activity exercised or the financial, economic and / or patrimonial situation of one's own and / or of any group to which it belongs; the power of representation, the identity of the signing delegates, the ownership or control structure.
- The customer uses identification documents that appear to be counterfeit.
- The customer is reluctant to provide or refuses to provide information, data and documents commonly acquired for the execution of the operation or for the settlement of services.
- The customer, upon exhibiting identity documents or upon requesting information on the operation or service, unreasonably renounces to perform it.
- The customer refuses to provide information on payment methods.
- The customer shows an unusual familiarity with the safeguards provided for by the legislation on customer due diligence, data recording and reporting of suspicious transactions, or asks repeated questions regarding the methods of application of these safeguards.
- The customer demonstrates that he does not have adequate knowledge of the nature, object or purpose of the professional service requested, raising the doubt that he can hide from acting with illicit purposes on behalf of a third party.
- The client is accompanied by other people - whose role has not been ascertained during contacts with the professional - who seem to have a direct interest in how to perform the service.
- The customer carries out transactions for a significant amount and is known to have been subjected to criminal proceedings, to preventive measures or to seizure orders, or is notoriously contiguous (for example family members) to subjects subjected to criminal proceedings, to preventive measures or to measures of seizure. seizure, or carries out transactions with counterparties known to have been subjected to criminal proceedings, preventive measures or seizure orders.
- The customer is registered, is notoriously contiguous (for example family member) to registered subjects or requests to carry out transactions with counterparties registered in the lists of persons or entities active in the financing of terrorism.

- The customer operates in countries with an anti-money laundering regime not equivalent to that of the countries of the European Community and requests or carries out the following operations, without providing reasonable reasons related to the activity carried out, to the group to which they belong or to particular conditions adequately documented:
    - constitution or transfer, in the aforementioned countries, of real rights over immovable property;
    - contribution for the establishment or capital increase - especially if carried out for large amounts - of companies that have their registered office in the aforementioned countries;
    - use, as shareholders, of companies set up as a trust in the aforementioned countries;
    - transfer of shareholdings or rights on quotas or shares, or on other financial instruments that give the right to acquire such shareholdings or rights, if a foreign subject is interposed with apparent dissimulation purposes; - receipt and / or transfer of funds.

Additionally, participants in the Seminar considered it advisable for any medium or other risk operation to do research in public and confidential data banks and ask for any other information or documentation that is deemed appropriate.

2. Mitigating vulnerabilities

The content of the second Seminar, held in Brussels, was the **"EU risk assessment methodology and EU and FATF Guidelines for Legal Professions"**, with the aim to gather best practices in **"Mitigating vulnerabilities"**.

Even the best practices were not gathered during the Seminar, the following is a summary of the content related to the vulnerabilities addressed during the Seminar, and the related best practices to mitigate them:

- General aspects related to the vulnerabilities.
- Services provided by lawyers that entail ML/TF vulnerabilities.
- Services provided by notaries that entail vulnerabilities on ML/TF.
- RBAs to assess vulnerabilities.
- Mitigating measures.
- General risky services:
    - Client funds.
    - Advising in the purchase/sale of real property.
    - Formation and management of companies and trusts.
    - Acting as a nominee.
    - General management of client affairs.
    - Other services that may indicate ML/TF.
- Client risk.
- Transaction risk.

2.1 General aspects related to the ML/FT vulnerabilities

Notaries and Lawyers face the risk to be used for money laundering and terrorist financing purposes for three main reasons:

- The intervention of a lawyer or a notary add respectability and an appearance of legitimacy
- Their expertise is useful/necessary
- They frequently handle client's money through client accounts

In this sense, they must understand the risks they are exposed to, and the techniques and mechanisms used by the criminals, identifying the most relevant vulnerabilities:

- How vulnerabilities can be taken as an advantage by criminals to infiltrate into the legal economic flow.
- Vulnerabilities that prevent the detection of the beneficial owner, as this is one of the issues detected in the "REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the assessment of the risks of money laundering and terrorist financing affecting the internal market and related to cross-border activities".
- Vulnerabilities in the identification of the intervening parts dealing with notaries and lawyers.

- Vulnerabilities in the understanding of the purpose of the business relation that the customers of notaries and lawyers are pretending to carry out.
- Vulnerabilities in the detection of suspicious transactions by notaries and lawyers.
- Vulnerabilities in the analysis of suspicious transactions by notaries and lawyers.
- Vulnerabilities in the internal management and reporting of suspicious transactions.
- Vulnerabilities on the collaboration by notaries and lawyers with local and international authorities.

2.2 RBAs to assess vulnerabilities.

As determined during the seminar, a risk-based approach is required prior to implementing AML/CTF measures. In regard to lawyers and notaries, this approach should include identifying and maintaining an understanding of the ML/TF risk faced by the sector as well as specific to their services, client base, the jurisdictions where they operate, and the effectiveness of their controls in place.

Additionally, further steps should be followed by:

- identifying and applying measures to effectively and efficiently mitigate and manage ML/TF risks.
- putting in place policies, procedures and information systems to monitor changes to ML/TF risks.
- documenting risk assessments, strategies, policies and procedures to monitor, manage and mitigate ML/TF risks.

2.3 General risky services.

In general, risky services for legal professionals identified during the Seminar are:

- Client funds.
- Advising in the purchase/sale of real property.
- Formation and management of companies and trusts.
- Acting as a nominee.
- General management of client affairs.

Additionally, participants in the seminar stated that, in some cases, client accounts are held by legal professionals with a financial institution. This service, which entails a clear ML/TF risk, usually includes the use of exclusive bank accounts and written requirements of management/disposal of such funds.

The use of client accounts has been identified as a potential vulnerability among the Seminar participants, as it may be perceived by criminals as a means to either integrate tainted funds within the mainstream financial system or a means by which tainted funds may be layered in such a way to obscure their source, with fewer questions being asked

by financial institutions because of the perceived respectability and legitimacy added by the involvement of the legal professional.

Participants agreed training on how to manage this service from an AML/CTF point of view is to be provided as a best practice. In general, the AML/CTF requirements for this service include:

- Sign a prior legal document detailing how the funds are to be managed.
- Keep written track of all funds managed, the transfers and who decided what upon which legal support.
- Close all relationships that entail this service which are dead or outdated.

Real estate, both commercial and residential, accounts for a high proportion of confiscated criminal assets, demonstrating that this as a clear area of vulnerability. In many countries, legal professionals are either required by law to undertake the transfer of property or their involvement is a matter of tradition, custom or practice. However, the specific role of legal professionals in real estate transactions varies significantly from country to country, or even within countries, as set forth by participants.

Highlight referred to the fact that some criminals may seek to invest the proceeds of their crime in real estate attempting to obscure their ownership of the real estate. Alternatively, criminals may seek to obscure the ownership of real property by using false identities or title the property in the names of family members, friends or business associates, or purchase property through an entity or a trust. Legal professionals should consider carefully who they are acting for at the outset of a real estate transaction, especially where there are multiple parties involved in a transaction. In some cases, legal professionals may also opt to apply specific checks on the settlement destinations of transactions.

Individuals may sometimes have lawyers or other persons hold their shares as nominees, where there are legitimate privacy, safety or commercial concerns. However, criminals may also use nominee shareholders to obscure their ownership of assets.

Lawyers should identify beneficial owners when establishing business relations in these situations. This is important to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the client to be able to properly assess and mitigate the potential ML/TF risks associated with the business relationship. Where lawyers are asked to act as nominees, they should understand the reason for this request and ensure that they are able to verify the identity of the beneficial owner of the shares and that the purpose is legitimate.

Remarks were made on access to beneficial ownership data bases, as well as examples of these data bases (Spanish example).

In some jurisdictions, lawyers may undertake a range of management activities for clients permitted in limited circumstances by some professional rules.

Situations where a lawyer may be undertaking these activities legitimately may involve a client who has limited capacity to manage his/her own affairs, or in other circumstances where the client has a clear legitimate rationale for seeking the continuing assistance from the lawyer.

Examples of these situations were discussed, how to proceed and how to keep record of the appropriate actions.

Additionally, risky services provided in Belgium, Bulgaria, Italy and Spain were discussed in relation to ML/TF. These included, but were not limited to, the following:

- The creation of financial instruments and arrangements.
- Advice on and drafting of contractual arrangements.
- The creation of powers of attorney.
- Probate (succession) and insolvency or bankruptcy work, specifically how to detect fictitious insolvencies originated to justify unlawful funds transfers

2.4 Services provided by lawyers and notaries that entail ML/TF vulnerabilities.

The following are examples of services provided by lawyers that were deemed with vulnerabilities during the seminar:

- Advising on the purchase, sale, leasing and financing of real property;
- Tax advice;
- Advocacy before courts and tribunals;
- Representing clients in disputes and mediations;
- Advice in relation to divorce and custody proceedings;
- Advice on the structuring of transactions;
- Advisory services on regulations and compliance;
- Advisory services related to insolvency/receiver-managers/bankruptcy;
- Administration of estates and trusts;
- Assisting in the formation of entities and trusts;
- Trust and company services;
- Acting as intermediaries in the trade of citizenship and residency or acting as advisors in residence and citizenship planning;
- Providing escrow services and token custody services in connection with legal transactions involving an initial coin offering or virtual assets;

Similarly, the following are examples of services provided by notaries where vulnerabilities were identified:

- Overseeing the purchase of shares or other participations.
- Legitimization of identities of signatory.
- Legalization of old documents.
- Opening of safe deposit boxes.

2.5 Client risk.

Determining the potential ML/TF risks posed by a client or category of clients was deemed critical to the development and implementation of an overall risk-based framework.

Categories of clients whose activities may indicate a higher risk were drawn as follows:

- PEPs and persons closely associated with or related to PEPs.
- Clients conducting their business relationship or requesting services in unusual or unconventional circumstances.
- Clients where the structure or nature of the entity or relationship makes it difficult to identify in a timely manner the true beneficial owner or controlling interests or clients attempting to obscure understanding of their business, ownership or the nature of their transactions. For example:
    - Unexplained use of shell and/or shelf companies.
    - Unexplained use of informal arrangements (family members).
    - Unusual complexity in control or ownership structures without a clear explanation.
- Client companies that operate a considerable part of their business in or have major subsidiaries in countries that may pose higher geographic risk.
- Clients that are cash intensive businesses, such as:
    - Money or Value Transfer Services.
    - Operators, brokers and others providing services in virtual assets.
    - Casinos, betting houses and other gambling related institutions and activities.
- Businesses that rely heavily on new technologies.
- Non-profit or charitable organizations engaging in transactions for which there appears to be no logical economic purpose.
- Clients using financial intermediaries, financial institutions or legal professionals that are not subject to adequate AML/CFT laws and measures.
- Clients who appear to be acting on somebody else's instructions.
- Clients reluctant to provide all the relevant information.
- Clients who appear to actively and inexplicably avoid face-to-face meetings.
- Clients who request that transactions be completed in unusually tight or accelerated timeframes.
- Clients with previous convictions for crimes that generated proceeds, who instruct legal professionals (who in turn have knowledge of such convictions) to undertake specified activities on their behalf.
- Clients who have no address, or who have multiple addresses.
- Clients who have funds that are obviously and inexplicably disproportionate to their circumstances.
- Clients who change their settlement or execution instructions without logic.

- Clients who change their means of payment for a transaction at the last minute and without justification.
- Clients who insist, without reasonable explanation, that transactions be effected exclusively or mainly through the use of virtual assets.
- Clients who offer to pay unusually high levels of fees for services that would not ordinarily warrant such a premium.
- Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile.
- The legal professional's client base includes industries or sectors where opportunities for ML/TF are particularly prevalent.
- Clients who apply for residence rights or citizenship in a jurisdiction in exchange for capital transfers.
- Clients who are suspected to be engaged in falsifying activities through the use of false loans, false invoices, and misleading naming conventions.
- The relationship between employee numbers/structure and nature of the business is divergent from the industry norm.
- Client seeking advice or implementation of an arrangement that has indicators of a tax evasion purpose.
- The transfer of the seat of a company to another jurisdiction without any genuine economic activity in the country of destination.
- Dormant clients who suddenly require services.
- Client that start or develop an enterprise with unexpected profile or abnormal business cycles.
- Indicators that client does not wish to obtain necessary governmental approvals.
- Reason for client choosing the legal professional is unclear.
- Frequent or unexplained change of client's professional representatives/managers.

2.6 Transaction risk.

The trainer in the Seminar highlighted that, in addition to client's risk, the transaction carried out by the client, and the service related, may also entail a ML/TF risk.

It was considered a best practice to pay attention to the following transactional risks for lawyers and notaries:

- Services where legal professionals, effectively acting as financial intermediaries, handle the receipt and transmission of funds through accounts they control.
- Services where the client may request financial transactions to occur outside of the legal professional's trust account.
- Services where lawyer may in practice represent or assure the client's standing, reputation and credibility to third parties.
- Services that are capable of concealing beneficial ownership from competent authorities.

- Services requested by the client for which the legal professional does not have expertise.
- Services that rely heavily on new technologies that may have inherent vulnerabilities.
- Transfer of real estate or other high value goods or assets between parties in a time period that is unusually short.
- Payments received from un-associated or unknown third parties and payments in cash where this would not be a typical method of payment.
- Transactions where it is readily apparent to the legal professional that there is inadequate consideration.
- Administrative arrangements concerning estates where the deceased was known to the legal professional as being a person who had been convicted.
- The use of shell companies, companies with ownership through nominee shares or bearer shares and control through nominee and corporate directors.
- Situations where advice on the setting up of legal arrangements may be misused to obscure ownership or real economic purpose.
- Services that have deliberately provided, or depend upon, more anonymity in relation to the client's identity or regarding other participants, than is normal.
- Settlement of default judgments or alternative dispute resolutions is made in an atypical manner.
- Use of virtual assets and other anonymous means of payment and wealth transfer within the transaction without apparent justification.
- Transactions using unusual means of payment.
- The postponement of a payment for an asset or service delivered immediately to a date far from the moment at which payment would normally be expected.
- Unexplained establishment of unusual provisions in credit arrangements that do not reflect the commercial position between the parties.
- Transfers of goods that are inherently difficult to value where this is not common for the type of client.
- Successive capital or other contributions in a short period of time to the same entity.
- Acquisitions of businesses in liquidation with no apparent purpose.
- Power of representation given in unusual conditions.
- Transactions involving closely connected persons and for which the client and/or its financial advisors provide inconsistent or irrational explanations.
- Unexplained delegation of authority by the client through the use of powers of attorney.
- Provision of registered office facilities and nominee directorships without proper explanations.
- Unexplained use of discretionary trusts.
- Unexplained relationship between a settlor and beneficiaries with a vested right in a trust.
- Services where the lawyer acts as a trustee/director that allows the client's identity to remain anonymous.

- Situations where a nominee is being used with no apparent purpose.
- Unexplained use of pooled client accounts or safe custody of client money or assets or bearer shares.

2.7 Mitigating measures.

Mitigating practices, upon comments during the Seminar, should invariably include initial and ongoing CDD, internal policies, training, and procedures to address the vulnerabilities faced in the lawyers' particular context. Legal professionals should take enhanced measures to manage the ML/TF risks identified.

In general, the mitigating measures should include:

- Client acceptance and know your client policies.
- Engagement acceptance policies.
- Understand the commercial or personal rationale for the work.
- Be attentive to red flag indicators.
- Then consider what action, if any, needs to be taken and have an action plan.
- Documentation.

During the Seminar, it was considered the approach to be followed, provided by the FATF recommendations to legal professions:

- **Client acceptance and know your client policies:** identify the client and its beneficial owners and the true "beneficiaries" of the transaction + where required, understanding of the source of funds and source of wealth and purpose of the transaction
- **Engagement acceptance policies:** understand the nature of the service provided (how the work of the professional could help to obscure the proceed of a crime?)
- **Understand the commercial or personal rationale for the work**
- **Be attentive to red flag indicators**
- **Then consider what action, if any, needs to be taken and have an action plan**: the level of risk will dictate the level and nature of the evidence/documentation to collect
- **Documentation**: it is essential for legal professionals to document all the steps they have taken in the fulfillment of their AML/CFT obligations.

Among the member countries, there are some AML/CFT systems in the legal professionals' sector, where the assessment of the sector's risk, the development of the policies and procedures for AML/CFT and the training of legal professionals are the responsibility of the Self-Regulatory Bodies, which guarantees homogeneity and uniformity in the requirements for the application of these policies throughout the 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.

3. Questing red flags

The content of the third Seminar, held in Sofía, was the **"Know Your Customer, Customer Due Diligence, Beneficial Ownership, Reporting Obligations, Records keeping, Evidence gathering and Regulatory Technology"**, with the aim to gather best practices in **"Questing red flags"**.

Keeping into consideration the scope of legal professionals' AML/CTF obligations, an empirical analysis was performed during the Seminar. To do so, three hypotheticals were developed to measure the awareness of both target groups (lawyers and notaries) of money laundering (ML) and terrorism financing (TF) red flags, and their ability to identify the beneficial owner(s)[1]. The participants split into mixed international groups, each group comprising lawyers and notaries from the three participating jurisdictions, namely Bulgaria, Italy and Spain.

Following group discussions, the participants shared their opinion on the identified red flags and problems in the manner in which the legal professional in the hypotheticals handled the scenarios. Each of the test groups was asked to identify the type of information a lawyer and a notary should request in light of their *gatekeeper* obligations for the identification of the beneficial owner(s) as well as the ML/TF red flags in these scenarios from both perspectives.

Before moving to the hypotheticals, it is important to be aware of the limitations of the applied approach. As the present report and the Seminar engage the inductive method, it draws a conclusion on ML red flags awareness among lawyers and notaries based on the results from the responses of the test group. However, the report recognizes that it bases its conclusions on a limited number of represented jurisdictions and a limited number of participants in the survey. As indicated, lawyers and notaries from the three EU Member states participated, with groups of six professionals from Italy, seven from Spain and thirty from Bulgaria.

3.1 Description of case studies

Case study nº 1

A law firm in the lawyers' respective jurisdiction is approached by Mr. John Smith, the CEO of Sandalwood Ltd, a legal entity incorporated in the United Kingdom. Mr. Smith would like the lawyer to represent Sandalwood Ltd in the purchase of an office building in her respective jurisdiction. To facilitate the purchase Mr. Smith suggests that 5 million EUR to be deposited to an attorney`s escrow account of the law firm. Mr. Smith apologizes that he is running behind his schedule and suggests that he provides any

[1] In developing the hypotheticals, the Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the Assessment of the Risk of Money Laundering and Terrorist Financing Affecting the Internal Market and Relating to Cross-Border Activities (SWD(2019) 650 final) was considered. Retrieved from https://eurlex.europa.eu/legal-content/BG/ALL/?uri=CELEX%3A52019SC0650 (last accessed on August 7th, 2022)

further information and documentation that may be needed by the law film in a few weeks when he will be back in the country.

As the law firm agrees to this arrangement, in a couple of days it receives the funds via wire transfer from the account of Transcontinental impex Corp. opened in the Commercial Bank of Moldova in Moldova. The negotiations for the purchase of the office building commence, yet the law firm receives new instruction from Mr. Smith. Now he wants the negotiations discontinued. He instructs the law firm to transfer 4 million EUR to the bank account of Overseas Media Ltd in the Bahamas. The remaining 1 million EUR is to be used for the purchase of an estate in the lawyer's jurisdiction for Ruselb Ltd recently registered in Armenia. At this point, Mr. Smith is yet to provide the needed information and documentation associated with the AML CDD.

To execute the client's instruction associated with the purchase of real estate, the law firm approaches a notary. In response to the notary's CDD inquiry, Mr. Smith provides the same response to both the notary and the law firm. He explains that the 5 million EUR is a Moldovan court default judgement in favor of Sandalwood Ltd on its case against Transcontinentalimpex Corp. He provides a translation of the first instance court judgement that has entered into force without being appealed. Mr. Smith notes that the follow-up transfers are associated with the business dealings of Sandalwood Ltd Mr. Smith notes that the 4 million EUR transfer to Overseas Media Ltd is associated with an "off-shore investment business transaction". On the purchase of the real estate for Ruselb Ltd, Mr. Smith notes that this is a payment on a consultancy contract for a public procurement secured by Sandalwood Ltd in Kazakhstan. According to the internet site of Ruselb Ltd is "specialized in government relations". However, the notary comes across a media publication that claims that "according to unconfirmed reports" the beneficiary owner of Ruselb Ltd is the daughter of the former president of the Republic of Kazakhstan.

In a nutshell, the case study presents a scenario in which the service rendered by the lawyer fall in the group most susceptible to ML - buying of real estate and movement of client's funds. It also features the elements of the global laundromat scheme (a.k.a. the Moldovan scheme or the Russian laundromat) and the use of lawyer accounts (escrow accounts) in the layering stage. It draws inspiration from the Statoil corruption scandal[2] in its last part. There are red flags associated with the type of business transactions, geographical RFs, and politically exposed persons (PEPs), among others. CDD and beneficial owner(s) identification are not done adequately.

Case study № 2

According to the second hypothetical Mr. Alfredo Donadoni, an Italian national, approaches a lawyer in the respective jurisdiction. Mr. Donadoni would like her to set

[2] More on the Statoil-Horton Case at ARMSTRONG, James. Statoil Settles With US For $21M In Iran Bribery Case. Law360. [online]19.11.20o9. Retrieved at https://www.law360.com/articles/135279/statoilsettles-with-us-for-21m-in-iran-bribery-case (last accessed on August 7th, 2022)

up a limited liability company. The scope of activity of the legal entity is the purchase and resale of vehicles and the import and export of vehicles. The capital of the legal entity is wholly owned by Oruzza Ltd, which is set up in Bulgaria. After the new legal entity, Amaranth Ltd is set up, Mr. Albertini, the CEO of this legal entity, asks the same legal professional to provide legal services for Amaranth Ltd regularly. As part of this arrangement, the lawyer becomes aware that Amaranth Ltd buys cars, trucks and other vehicles that are then shipped to Pakistan. In many instances, the cars are invoiced to a different customer than Amaranth Ltd. The majority of sales are made in cash. Most purchase invoices are below 10 000 EUR. It becomes known to the lawyer that in some instances the invoice price is "adjusted", as Mr. Donadoni puts it, "to reduce the tax burden on the local businesses which are hard-pressed due to economic hardship".

At one point Mr. Donadoni informs the lawyer that Oruzza Ltd is set to buy an apartment in the respective jurisdiction that will be used by the CEO of Amaranth Ltd. He asks for the legal services of the lawyer in the preparation of necessary paperwork and performing the ownership checks. Mr. Donadoni and the seller make an appointment with a notary. Mr. Donadoni and the seller declare that the purchasing price of 150 000 EUR is paid in advance and in full. According to the ownership title, the property was acquired by the vendor 4 years earlier for 250 000 EUR

In response to the CDD inquiry, Mr. Donadoni provides information from the Bulgarian Business Register according to which Oruzza Ltd is primarily dealing with import and export but has a very broad scope of activities. Its registered capital is 1 Euro, the minimum required by Bulgarian law. There are two stakeholders in Oruzza Ltd – one limited liability company incorporated in Switzerland and one limited liability company set up in Mauritius. Unofficially, the seller discloses to the notary that Mr. Donadoni offered the owner of the apartment to pay the asking price for the purchase fully in cash at the time the contract is signed. Further, he asks whether the seller would be willing to report a price that is below the actual price, noting that the seller will reduce tax dues. To facilitate the consent, Mr. Donadoni paid all expenses associated with the deal. The owner agreed.

In a fashion similar to the first hypothetical, this case study illustrates lawyer services listed by the FATF as prone to ML – establishment of a business legal entity and buying of real estate. There are some indicators of trade-based ML through under-invoicing, smurfing, RFs associated with the type of business transactions as well as countryspecific RFs concerning the business transactions. CDD and beneficial owner(s) identification leave much to be desired. The case also tests the inclination of the group to use open sources in the "know your customer" (KYC) process, namely whether participants would review a foreign business registry – information that is available online - as part of the initial KYC check.

Case study №3

According to the third hypothetical, Mr. Richard Deng, a French-South Sudanese national approaches a lawyer in the respective jurisdiction. Mr. Deng is the head of a

French non-profit organization "Food for the Children of the World". He explains that the organization collects donations to buy food and medical supplies that are then shipped to poverty and conflict-stricken countries that cannot guarantee the food security of children. Mr. Deng notes that the organization is ready to make three major shipments to three different countries in a short time. As this is a new and small organization it lacks the expertise and staffing to handle the task. It would like to secure the services of a legal professional for assistance with the transactions. Mr. Deng notes that the actual arrangements are in place but they need assistance with the legal aspects of those. The three transactions are as follows:

- 10 000 tons of wheat from Dubai to Iran;
- 50 tons of medications for Egypt to South Sudan, and,
- 10 000 tons of rice from Nigeria to Guinea.

The lawyer noted that according to the provided scanned fax offer the ship that was to transport the wheat has a carrying capacity of 5 000 tons. Mr. Deng noted that this is due to the low tonner of their fax machine and the actual capacity of the vessel is 15 000 tons. According to the documents provided, a Turkish precious metal and stones dealer finances the Iranian transaction through transfers from his bank accounts in Turkish banks. The lawyer notes that the medications for South Sudan are contributions from charitable organizations and individuals. Most of them are in-kind donations, rather than funds. Insignificant monetary donations are made to the bank account of "Food for the Children of the World" in France.

Mr. Deng informally shares with the lawyer that the transfer to Guinea is affected by logistical problems. Eventually, Mr. Deng, who is to accompany the shipment to South Sudan, gives the lawyer the power of attorney for the funds in the "Food for the Children of the World" account earmarked for Guinea. A day later Mr. Deng calls from Egypt. Mr. Deng tells the lawyer that the Guinea shipment is off and there will be follow-up instructions via e-mail. Via e-mail, Mr. Deng instructs the lawyer to return the money earmarked for Guinea to the donor. He notes that the funds are to be sent to a bank account of Mr. M. C. (in the actual case the name of an individual from the EU Commission Sanction List was used) in Mauritius. The lawyer notes that the funds came from a bank account of a limited liability company in France. This account is now closed. This case drew focus on the susceptibility of non-government organizations (NGOs) to ML. Again, a legal professional is involved in the management of business transactions for the client. The case draws inspiration, in part, from the Halkbank scandal case[3] , which features ML RFs associated with unusual business transactions. The case emphasizes the importance of open source intelligence sources. On the one hand, it uses Mauritius, which is on the FATF grey list, the EU high-risk third countries and the Organization for Economic Co-operation and Progress (OECD) lists with deficiencies in

[3] See (2019) Indictment of the U.S. Attorneys for the Southern District of New York, United State District Court which charged Halkbank with fraud, AML, and sanctions offenses in a scheme to evade U.S. sanctions on Iran. Retrieved from https://www.justice.gov/usao-sdny/pressrelease/file/1210401/download (last accessed on August 7th, 2022).

the AML regime, removed from each respectively in 2021 and 2022, to assess whether the test groups reference these instruments in the CDD process. Moreover, through Mr. M. C., whose full name appeared in the actual case and who is listed in the EU Commission Sanction List (https://sanctionsmap.eu/), made a similar evaluation. As in the other two cases, there are indicia CDD and beneficial owner(s) identification deficiencies. Thus, the case studies strive to assess empirically the effectiveness of lawyers and notaries as AML "gatekeepers" in two key aspects – red flags identification and beneficial owner(s) detection.

3.2 Crucial red flags identified

Upon the aforementioned case studies, the following red flags were identified during the seminar:

Chart 1. Summary of crucial red flags identified per case study.

IDENTIFIED RED FLAGS	CASE STUDY 1	CASE STUDY 2	CASE STUDY 3
KNOW YOUR CLIENT PROCEDURES	Some weaknesses and shortcomings are detected. ILPs neglect some mandatory procedures on account of fast and timely legal services provision. Some notaries (Spain) reported that in case of a suspicious client, they`re not allowed to refuse a notary service but are obliged to report it, immediately.		
CLIENT DUE DILIGENCE	Some weaknesses and shortcomings are detected. ILPs immediately identify the necessary documents, evidence and procedures regarding CDD and KYC performing adequate checks but some of them forget to ask the client for submission, thereon. A common mistake by some ILPs (Bulgaria) is not getting a copy of the client`s official identity document[4]. Some ILPs declare avoidance of verification activities within (pre)paid commercial database sources and public registries (open-data sources) with membership accounts due to additional costs and insufficient budget.		
IDENTIFICATION OF BENEFICIAL OWNER(S)	ILPs demonstrate a good level of knowledge on the BOs role in the ML/TF process but perform some checks partially without a thorough investigation on control levels through owner`s shares or interests, due to lack of time (according to respondents). Some ILPs trust the Register of BOs without any additional verifications performed. Exhaustive BOs examinations could be performed upon a senior management order. Several difficulties are observed in the case of ultimate beneficial owners' identification.		

[4] Administrative Penalty Provisions pursuant to Art. 53, para. 1 of the Measures against Money Laundering Act (Bulgarian jurisdiction). Promulgated, SG No. 27/27.03.2018, amended supplemented, SG No. 32/26.04.2022 effective 27.07.2022. Retrieved from https://www.dans.bg/en/msip-091209-menu-en (last accessed on August 7th, 2022).

IDENTIFIED RED FLAGS	CASE STUDY 1	CASE STUDY 2	CASE STUDY 3
BUSINESS TRANSACTION TYPE	ILPs demonstrate a good level of knowledge of business transaction types and easily detect them. They can list the key elements of the transaction structure, the value chain within it and several documents associated with it. Based on their experience and market practices, they immediately could detect possible suspicious behavior and potential ML/TF schemes. ILPs are familiar with and identify correctly several risky and suspicious businesses and business transaction types.		
LEGAL ENTITIES	ILPs perform excellent execution of legal entities identification and classification concerning simplified or enhanced CDD. They apply a special approach to business entities and PEPs especially associated with geographic and country risks (see below). Sanctions Lists checks are performed with some exclusions.		
POWER OF ATTORNEY	N/A	N/A	ILPs detect correctly the obligation to immediately verify the power of attorney and identify the proxy before entering into business relations. They explain various ways of verification within their domestic legislation. They associate the power of attorney with potential risks.
GEOGRAPHIC & COUNTRY RISKS	ILPs demonstrate a highly developed sense of potential geographic and country risks associated with the related clients and transactions. They are very keen on countries' classification regarding AML/CTF activities (third countries, High-Risk third countries & jurisdictions, black/grey list countries, etc.). They make a difference between “a country” and “a jurisdiction” concerning AML/CTF process. ILPs follow updates on different Black/Gray List or High-Risk Third Countries.		
	The United Kingdom is detected as a third country (after Brexit). Moldova, Bahamas and Kazakhstan are also accurately and timely detected.	Pakistan and Mauritius are accurately and timely detected. Some suspicions and assumptions are performed.	All countries and jurisdictions involved in are subject to additional checks for various geographic and country risks.

IDENTIFIED RED FLAGS	CASE STUDY 1	CASE STUDY 2	CASE STUDY 3
OFFSHORE FINANCIAL CENTRES (ZONES)	ILPs possess in-depth knowledge of offshore areas and jurisdictions worldwide and are able to identify them immediately by associating relevant ML/TF risks and threats. A client, a business entity or a transaction from/to offshore zones/jurisdiction are classified as high-risk one(s). ILPs detect a relation between offshore zones` risks and geographic & country risks, in general.		
CURRENCY RISK	N/A	ILPs identify the Pakistani rupee as a potential non-convertible currency, thus a risky one. In fact, it is a convertible to the U.S. dollar since 1971. The case here shows a stressed focus of ILPs on potential ML/TF operations.	N/A
CASH RISK	N/A	ILPs identify cash payment as a risky one even below the regulatory thresholds. They do not accept it in international cross-border business and personal payments and determine it as an unreasonably high risk.	N/A
POLITICALLY EXPOSED PERSONS CHECKS	In principle, ILPs are very well familiar with different PEPs Lists both at the domestic and the EU level. They respond that they perform an enhanced CDD on a regular base. Concerning the three case studies, ILPs failed to detect some of the PEPs perhaps due to lack of time or stress or neglected details from the descriptions.		

IDENTIFIED RED FLAGS	CASE STUDY 1	CASE STUDY 2	CASE STUDY 3
	ILPs are not able to detect the daughter of the former President of Kazakhstan as a PEP. No additional information was provided regarding the end of the President`s term (a period after it).	N/A	N/A
SANCTIONS LISTS CHECK	In all the three examined cases ILPs preferred to rely on presented documents by the tutors and facts declared by a client instead of performing their own independent check in different public sanctions databases and taking into consideration the crucial information delivered by the EU Commission, the U.S. OFAC, the U.S. Treasury Department, as well as the United Nations Security Council and other international bodies via their public Sanction Lists.		
USAGE OF ESCROW (LAWYERS' AND NOTARIES') ACCOUNTS	ILPs detect correctly escrow accounts as suspicious and risk payment behavior. They prefer to refuse such transactions and terminate the business relationship with the customer.	N/A	N/A
REPORTING SUSPICIOUS TRANSACTIONS & CLIENTS	Based on different suspicious transactions and clients detected during the three investigated hypotheses, all ILPs declared readiness to perform an immediate reporting procedure under domestic legislation rules before the competent national authority. Some ILPs add that they must fill out their Journals on Suspicious Transactions and Clients and ask for an opinion from the senior management (in the case of law firms). A minority reports that they would prefer to fill out the Journal keeping the statement that a notification to the competent national authority is not necessary because they do not wish to enter into a relationship with a supervision body.		

IDENTIFIED RED FLAGS	CASE STUDY 1	CASE STUDY 2	CASE STUDY 3
DIFFERENT PRICE CORRECTIONS	N/A	ILPs identify any price corrections as a potential suspicious behavior for the purpose of illicit flow concealment or tax invasion.	N/A
ALL TYPES OF IN-KIND DONATIONS	N/A	N/A	Nevertheless, its types, forms and amounts, all in-kind donations are detected by ILPs as suspicious transactions. In combination with the NGO status of the related party subject to the transaction, those types of donations and sponsorships increase the risk score of the financial operation performed by any ILP. Therefore, it should be terminated.

Source: self-developed by seminar participants upon workshops at the Sofia Seminar.

The test group of legal professionals` results demonstrate that, in general, lawyers and notaries have reasonable knowledge of red flags. They are well aware of their obligations to perform CDD before accepting a customer and establishing a business relationship. They immediately identify the inadequate CDD clearly stating that if at the outset the customer de facto declines to provide the necessary information, this customer shall not be accepted. The discussion on the associated costs demonstrated that notaries, for example, did not discuss the need for performing the task. They recognize that they carry out a public function. Yet, the Bulgarian notaries raised the issue that, unfortunately, the customer bears this extra cost associated with the process. The Italian notaries, in particular, reported that national sanctions for non-performance of an initial CDD in the first hypothetical are effective and dissuasive. As for the time to execute such a check, Spanish notaries indicated that they benefit from an internal system accessible to all notaries in Spain that positively affects the timely performance of the CDD and beneficial owner checks.

The legal professionals demonstrated the ability to identify red flags associated with business transactions and practices. They immediately pinned down the invoice interference, documentation discrepancies and unjustifiable and illogical claims for price volatility in the case studies as red flags. Further, goods originating from business relationships with industries that are known not to be consistent in accurately documenting their transactions raised reasonable suspicion on behalf of the test group. It indicated that second-hand car sales, consistently at values under the reporting threshold, call for further review, especially in combination with the transaction destination being a FATF Grey List jurisdiction.

The legal professionals even identified the business relationship as a potential Black-Market Peso Exchange. Similarly, the discrepancy in tonnage of the vessel and the claimed volume of transported goods, as well as the communication method, raised suspicion and prompted further inquiry on the origin of the wheat, as Dubai is not known to be a wheat exporter.

They deftly identified unusual payment or money transfer arrangements that raise suspicion. The participants unanimously deem any client requests to use a lawyer's escrow accounts as a red flag. In fact, the majority of the test group indicated that such a request would make them reluctant to take the client or would bring the business relationship with such a client to an end. Further, money transfers to accounts unassociated with the client as well as instructions to transfer funds to accounts that are not associated with the account from which the funds originated raised concerns among the group. The response was that such instructions should not be followed.

Interestingly, the legal professionals seemed to be inclined to broaden the geographical scope of jurisdictions that raise suspicion. Further, if a jurisdiction appeared recently in the FATF Gray List or the EU High-Risk Third Countries Having Strategic Deficiencies in their Regime on AML and Countering the Financing of Terrorism, even after its removal from the list, the reputational damage seems to linger among some riskaverse lawyers. The reason for such an approach on behalf of the test group may be partially due to the number of different lists, which demonstrate nuances in their content. Such are the FATF Black and Grey Lists and the EU High-Risk Third Countries Having Strategic Deficiencies in their Regime on AML and Countering the Financing of Terrorism.

However, the group encounters challenges in the personal red flag rubric. Part of that is associated with the fact that various lists have a direct and indirect effect on this matter. In this vein, a lawyer would de facto need to take into consideration the U.S. Office of Foreign Sanctions Control (OFAC) Sanctions list as financial institutions will decline to take as customers listed individuals. Additionally, legal professionals need to consider at least European Commission Sanctions List and respective national PEPs lists. The other difficulty is the identification of ultimate beneficial owners, particularly when it comes to legal entities. Such challenges are not idiosyncratic to the legal profession, and it comes as no surprise that FATF amended its recommendation 24 in March 2022 to strengthen this aspect of the AML regime.

There is a nexus between the above issue and the lack of routine among legal professionals to consult publicly accessible online official registries and databases in other jurisdictions. The legal professionals did not attempt to confirm for themselves the incorporation of Oruzza Ltd in the Commercial Register of Bulgaria[5], choosing to rely on a document presented by a client that has a track record of "adjusting" documents. Similarly, the test group did not check Mr. M. C. and remained oblivious that he appears on the European Commission Sanction List.

The most problematic matter seems to be tackling ML/TF schemes backed by judicial decisions or arbitration awards. As lawyers are to recognize judicial decisions and arbitration awards as legitimate and legal unless explicitly challenged by the parties, the global laundromat scheme per se did not raise any issues associated with the substance of the scheme. Test group lawyers were concerned with the geographical factors, preceding transactions, etc. but not the gist of the scheme. This is understandable as lawyers are not in a position to subject the court case on which a final decision is rendered for potential simulation[6].

One can recapitulate the above findings as acute red flag sensitivity v. moderate ultimate beneficial owners' detection. In general, test group lawyers demonstrate serious "red flags" sensitivity. This is particularly true when it comes to less complicated or moderately complicated ML schemes. In complex ML schemes, particularly those involving final judicial decisions that have entered into force lawyers' commitment to recognizing the decision overrules ML suspicions. In the identification of beneficial owners, lawyers encounter challenges that are characteristic across the board. Many of these are due to objective difficulties.

Based on the above, on the way forward, lawyers and notaries, as well as other legal professionals, have an important role to play as AML "gatekeepers". The effective application of the regime should be the focus as the knowledge of the usual manner in which business transactions are executed, and ordinary payment mechanisms, among others, make lawyers capable of detecting uncommon practices and performing inquiries by having access to key documents that make detection of ML likely. Understandably, their effectiveness has its limitations partly due to objective obstacles.

3.3 Best practices

The following best practices were identified during the Seminar:

[5] Retrievedfrom https://portal.registryagency.bg/en/commercial-register.

[6]

8 Similar issues with variations detected in other studies on this matter. See HELGESSON, K. S., Ulrika Mörth. Client privilege, compliance and the rule of law: Swedish lawyers and money laundering prevention. Crime Law Soc Change 69, 227–248 (2018). Retrieved from https://doi.org/10.1007/s10611-017-9753-8, (2018). (last accessed on August 7th, 2022)

Chart 2. Summary of good market practices identified within the experience-sharing session.

IDENTIFIED RED FLAGS	GOOD MARKET PRACTICES (SOLUTIONS OF QUESTING RED FLAGS)
KNOW YOUR CLIENT PROCEDURES	• Open-source intelligence & paid database; • International journalists' investigation; • Networking, club memberships & references; • Taylor-made questionnaires and survey forms; • Additional information provided by other ILPs/obliged entities; • Court/Prosecutor decisions; • Clean driving license; • Police records; • Public activities: interviews, publications, social responsibility, blogs/vlogs/personal websites, social media, public lectures, master classes etc.; • Medical/Health statements and laboratory results; • Family status & Personal life information; • Risk assessment methodology under the FATF Recommendations[7];
CLIENT DUE DILIGENCE	• Personal identity documents verification in an open database (Ministry of Interior, Consular Section); • Verification by bank/insurer/Social, Healthy & Pension Funds; • Verification based on certificates and other relevant documents issued by an employer; • Verification based on Public registers database: Commercial Register, NGOs Registry, Property Registry, Spouses` Property Relations Registry, Register of providers engaged in exchange services between virtual currencies and fiat currencies, Custodian wallet providers registry, Central Credit Register, Register of Bank Accounts & Safe Deposit Boxes, Register of Operators of Payment Systems, Register of the licensed payment institutions on the territory of a state, as well as their branches and agents, Register of the licensed electronic money institutions on the territory of a state as well as their branches and agents, Register of the Payment Services and Payment Systems providers, Credit Intermediaries Register, Register of persons who may act as tied agents, Register of data reporting service providers, Register of multilateral trading facilities, Register of the European Banking Authority, Insurance agents and ancillary insurance intermediaries Registry and other centralized registers; • Verification is based on Information provided by real estate agencies/agents, auditors, accountants, tax advisors etc.;

[7] FATF (2019), Guidance for a Risk-Based Approach for Legal Professionals, FATF, Paris, France. Retrieved from www.fatf-gafi.org/publications/documents/Guidance-RBA-legal-professionals.html (last accessed on August 7th, 2022).

IDENTIFIED RED FLAGS	GOOD MARKET PRACTICES (SOLUTIONS OF QUESTING RED FLAGS)
IDENTIFICATION OF BENEFICIAL OWNER(S)	• Investigation and market research of complex and long value chains or ownership (direct/indirect ownerships), multiple layers of ownerships between assets and (ultimate) beneficial ownership(s) including within different jurisdictions and states; • Investigation and market research on "SHELL", "SHELF" & "FRONT" companies; • Survey on cases with a dispersion of company establishment, registration, residence and assets management in different jurisdictions; • Extensive exploration of public information stored at the Registry of Beneficial Owner(s); • Exploration of close family, business and political relationships and contacts among potential (ultimate) beneficial ownership(s); • Reasonable conclusions based on public shared information and confessions by potential (ultimate) beneficial ownership(s): interviews, briefings, press conferences etc.; • Investigation of bearer shareholdings and negotiable instruments & bearer shareholdings warrants, formal/ informal nominee shareholders & directors; • Verification of Declaration by multiple beneficial owners and/or multiple holders on the same bank account; • Manipulated company prospects, annual/semiannual financial reports etc.;
BUSINESS TRANSACTION & RELATIONSHIP TYPE	• Survey on client motivation regarding the background and the business purpose of establishing business transaction/relationship type: inducements, expected/intended/desired outcomes and results, personal preferences & abilities, patterns of transactions etc.; • Historical review of previously established and closed business transactions/relationships and reasons for closing them;
POWER OF ATTORNEY	• Immediate check-in notarial registers; • Sharing experience with other obliged entities and check in at their database; • Primary graphological expertise regarding the authenticity of signatures (in case of suspicions); • Check-in of any time constraints on power of attorney (valid until/after a certain day and time, jurisdiction, state, special conditions etc.);
GEOGRAPHIC & COUNTRY RISKS	• Check in periodically of the FATF grey list, the EU high risk third countries and the OECD lists for any updates; • Risk allocation and risk appetite assessment based on a survey of concrete countries (jurisdictions) and geographic regions;
OFFSHORE FINANCIAL CENTRES (ZONES)	• Check-in periodically of Offshore Islands, Countries, Territories, and Lists for any updates; • Focus on coverage geography; • Investigation of open databases with (de)classified information ("Panama Papers", "Pandora Papers", "Wikileaks", "Swissleaks") etc.; • SWOT analysis of business advantages and benefits; • Reviews on online images and maps (Google maps, Google Street);

IDENTIFIED RED FLAGS	GOOD MARKET PRACTICES (SOLUTIONS OF QUESTING RED FLAGS)
CURRENCY RISK	• Check-in periodically of Freely Convertible Global Currency Lists for any updates (delivered by the International Monetary Fund); • Country Analysis on potential risks associated with a concrete country, jurisdiction or region and its currency; • Currency arbitrage and hedge investment operations, ETFs, futures, options etc.;
CASH RISK	• Compliance with thresholds under *acquis communautaire* and local cash payment restriction acts;
POLITICALLY EXPOSED PERSONS CHECKS	• Check-in periodically of PEPs Lists for any updates; • Compulsory check-in procedures after each political election for any updates; • Actualization by accident 1 month after the first actualization; • A clear distinction between different PEPs, their family members and persons are known to be close associate with them; • Identification/Verification by compulsory declaration; • Check-in within internal/external public databases (websites of governmental institutions, courts, international organizations etc.); • Reputation risk check-in by open intelligence source database; • Following personal interviews, publications, social media, and blogs for relative information; • Sanctions Lists check-in; • Analysis of Anti Bribery, Corruption & annual Taxes Declarations; • Analysis of real estate and funds; • Reference Letters by a governmental institution, political party, diplomatic mission, international organization etc.; • Report on Family Status and Relatives List (by public databases); • Report on Chosen Mode of Spouses` Property under the Spouses` Property Relations Registry;
SANCTIONS LISTS CHECK	• The Consolidated list of persons, groups and entities subject to EU financial sanctions; • The Office of Foreign Assets Control (OFAC) U.S. Treasury Department Sanctions List; • The United Nations Security Council Consolidated Sanctions Lists (Specially Designated Nationals List, Consolidated Sanctions List & Additional OFAC Sanctions List); • Sanctions adopted by the EU Commission following Russia's military aggression against Ukraine;
USAGE OF ESCROW (LAWYERS` AND NOTARIES`) ACCOUNTS	• Limitations on cases when escrow accounts are used on an initiative of clients; • Sharing/outsourcing of some types of trust management activities with credit institutions (in case of utilities, taxes, property management and other similar payments); • No refunds on previous clients' transfer payments to escrow accounts; • Survey of clients` appetite for escrow accounts usage instead of other trust management channels (credit institutions, payment/settlement agents, depositories/repositories, property management companies, real estate investment funds, special investment purpose companies & funds etc.;

IDENTIFIED RED FLAGS	GOOD MARKET PRACTICES (SOLUTIONS OF QUESTING RED FLAGS)
REPORTING SUSPICIOUS TRANSACTIONS & CLIENTS	• Help desk and contact points (Spanish notaries practice); • Notification of competent national supervisory authority for the contact person(s) regularly and per local jurisdiction rules and terms; • Technical check-in of all communication means/ protocols (e-signature, cloud spaces, encrypted protocols, cyber security rules and business continuity management rules etc.) regularly; • Summary of all relevant information, documents and pieces of evidence regarding suspicious transactions/clients including photocopies; • Keeping memos/protocols of any suspicions and uncertainties regarding client`s behavior or unusual transactions;' • Keeping a journal of suspicious transactions/clients up to date.

Source: self-developed by seminar participants upon workshops at the Sofia Seminar.

4. New crypto crimes

The content of the last Seminar, held in Madrid, was **"Virtual currencies, electronic money, business relationship without intermediaries and ML/FT risks"**, with the aim to gather best practices in **"New crypto crimes"**.

The following best practices were gathered during the Madrid Seminar in relation to a series of issues which are detailed below.

4.1 How to conduct CDD

Regardless of the nature of the relationship or Virtual Asset (VA) transaction, obliged entities should have in place CDD procedures that they effectively implement and use to identify and verify on a risk basis the identity of a customer, including when establishing business relations with that customer; where they have suspicions of ML/TF, regardless of any exemption of thresholds; and where they have doubts about the veracity or adequacy of previously obtained identification data.

Obliged entities, in conducting CDD to fulfill their obligations, should obtain and verify the customer identification/verification information required under national law. Typically, required customer identification information includes information on the customer's name and further identifiers such as physical address, date of birth, and a unique national identifier number (e.g., national identity number or passport number). Depending upon the requirements of their national legal frameworks, obliged entities are also encouraged to collect additional information to assist them in verifying the customer's identity when establishing the business relationship (i.e., at onboarding); authenticate the identity of customers; help determine the customer's business and risk profile and conduct ongoing due diligence on the business relationship; and mitigate the ML/TF risks associated with the customer and the customer's financial activities.

Based on a holistic view of the information obtained in the context of their application of CDD measures—which could include both traditional information and non-traditional information as described above—obliged entities should be able to prepare a customer risk profile in appropriate cases. A customer's profile will determine the level and type of ongoing monitoring potentially necessary and support the obliged entity's decision whether to enter into, continue, or terminate the business relationship. Risk profiles can apply at the customer level (e.g., nature and volume of funds, origin of virtual funds, etc.) or at the cluster level, where a cluster of customers displays homogenous characteristics (e.g., clients conducting similar types of VA transactions or involving the same VA). Obliged entities should periodically update customer risk profiles of business relationships in order to apply the appropriate level of CDD.

Obliged entities that engage in covered VA activities may adjust the extent of CDD measures, to the extent permitted or required by their national regulatory requirements, in line with the ML/TF risks associated with the individual business relationships, products or services. Obliged entities must therefore increase the amount

or type of information obtained or the extent to which they verify such information where the risks associated with the business relationship or VA activities is higher. Similarly, obliged entities may also simplify the extent of the CDD measures where the risk associated with the business relationship of activities is lower. However, obliged entities may not apply simplified CDD or an exemption from the other preventive measures simply on the basis that natural or legal persons carrying out the VA activities or services on an occasional or very limited basis. Further, simplified CDD measures are not acceptable whenever there is a suspicion of ML/TF or where specific higher-risk scenarios apply.

4.2 Practical implementation of CDD in relation to Virtual assets

The CCD of the legal professionals must focus on the identification of the beneficiary of the operation, as well as on establishing the legitimate origin of the funds. Notaries/lawyers should ask their customer to prove the ownership of the funds, and do, when possible, some verification of the information provided by their customers.

In relation to the existence of the funds, if they are located at a certain address provided by the client, it can be verified by consulting the blockchain. However, if the funds are in a centralized Virtual Assets Service Provider (VASP) that correctly applies CDD, it could be possible to request some type of certificate from that company on the existing balance in the client's account.

In relation to the funds belonging to the client, and if the funds are deposited in these reliable VASPs, a legal professional could also request some type of certificate to that VASP regarding the owner of these funds.

In case that the funds are deposited in non-hosted wallets, the mere possession of the private key only indicates that the person who possesses it really has access to the funds, and this case could be assimilated to the person who presented a large amount of cash to carry out the operation. However, on contrary to that analogy, another person from elsewhere could also access the funds if he had a copy of that private key.

If the justification for holding these funds was in a specific blockchain transaction, it must be necessary to verify that the operation has really been carried consulting the blockchain directly through a blockchain explorer, and the number of confirmations that it would have had. Usually, it is needed 6 confirmations to consider it immutable, and in this double spending of funds is avoided.

In relation to the source of funds, although a basic study can be carried out on the activity generating these funds, for legal professionals having a high number of employees, specific blockchain analysis tools are necessary to be able to carry out a more detailed verification of the origin by carrying out a traceability study. If a centralized VASP has been used by the client, it can provide additional information about their source.

Additionally, for smaller legal professionals, it would be advisable to ask the customer to provide documentation to justify the source of the funds used to obtain the VA.

4.3 Enhanced and simplified CDD

There are circumstances where the ML/TF risk is higher and where enhanced CDD measures must be taken. In the context of VA related activities, for example, it is deemed as best practice to consider the country or geographic specific risk factors. VASPs located in or VA transfers from or associated with certain countries present potentially higher risks for ML/TF.

While there is no universally agreed upon definition or methodology for determining whether a jurisdiction, in which a VASP operates or from which VA transactions may emanate represents a higher risk for ML/TF, the consideration of country-specific risks, in conjunction with other risk factors, provides useful information for further determining potential ML/TF risks. Indicators of higher risk include:

- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations operating within them.
- Countries identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking, smuggling, and illegal gambling.
- Countries that are subject to sanctions, embargoes, or similar measures issued by international organizations such as the United Nations.
- Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by the FATF statements as having weak AML/CFT regimes, especially for VASPs, and for which VASPs and other obliged entities should give special attention to business relationships and transactions.

Legal professionals should take into account the profile of the customer identifying high risk activities such as dividing large amounts into smaller ones, quantities just below threshold, operate with large amounts just after creating the account, or after a period of inactivity and then withdraw the funds, or use VASPs for illogical activities such as deposit and right after withdrawing.

Other kind of red flag indicators are: use of different VASPs, especially high risk VASPs, use of mixers, crypto Automated Teller Machine (ATM´s), Peer-to-Peer platforms to obtain VA, exposure to darknet markets, online gambling platforms or to criminal activities such as frauds, scams, or ransomware attacks.

In these and other cases, the EDD measures that may mitigate the potentially higher risks associated with the aforementioned factors include:

- Corroborating the identity information received from the customer, such as a national identity number, with information in third-party databases or other reliable sources.
- The use of analysis products, such as blockchain analytics to see the exposure of the addresses involved, track the origin of the funds, the operational (use of different VASP, especially high risk VASP, use of mixers, smurfing techniques, exposure to darknet markets or to criminal activities…), and hence assess the risk of the client.
- Searching the Internet for corroborating activity information consistent with the customer's transaction profile, provided that the data collection is in line with national privacy legislation.

Legal professionals should also consider other EDD measures such as obtaining additional information on the customer and intended nature of the business relationship, obtaining information on the source of funds of the customer, obtaining information on the reasons for intended or performed transactions, and conducting enhanced monitoring of the relationship and transactions.

In addition, they may also collect additional information on high-risk customers and transactions in order to identify, and avoid engaging in, prohibited activities, and to enable follow-up actions in a Risk-based approached (RBA) manner. Such additional information may include:

- The purpose of transaction or payment.
- Details about the nature, end use or end user of the item.
- Proof of funds ownership
- Parties to the transaction and the relationship between parties.
- Sources of wealth and/or funds, including justification of the salary / business which justify the origin of the funds.
- The identity and the beneficial ownership of the counterparty.
- Export control information, such as copies of export-control or other licenses issued by the national export control authorities, and end-user certification.
- Electricity and hardware bills in the case of mining.

Regarding a possible request for custody of funds by a client to the notary or lawyer, it must be taken into account that it can only be ensured if the notary or lawyer is the only one who knows the private key of the address where the funds are deposited (it should be under an address controlled by the custodial), and be sure that indeed the funds have been received into that address (that the transaction is confirmed).

Regarding the operations in which a notary is required to attest to the value of a certain wallet at a certain time, it can be done consulting directly the blockchain, but bearing in mind that the equivalent value in fiat fluctuates substantially.

Regarding the launch of new cryptocurrencies or initial coin offering (ICO), they must be subject to the advertisement conditions established in the legislation, as well as in the

future European MiCA law, but it is not established that they must be submitted in front of a notary.

4.4 Record-keeping

Legal professionals should maintain all records of transactions and CDD measures for a certain legal time frame in such a way that individual transactions can be reconstructed, and the relevant elements provided swiftly to competent authorities. Legal professionals engaging in VA activities should maintain transaction records on transactions and information obtained through CDD measures, including: information relating to the identification of the relevant parties, the public keys (or equivalent identifiers), addresses or accounts involved (or equivalent identifiers), the nature and date of the transaction, and the amount transferred, for example. The public information on the blockchain or other relevant distributed ledger of a particular VA may provide a beginning foundation for recordkeeping, provided institutions can adequately identify their customers. However, reliance solely on the blockchain or other type of distributed ledger underlying the VA for recordkeeping is not sufficient.

For example, the information available on the blockchain or other type of distributed ledger may enable relevant authorities to trace transactions back to a wallet address, though it may not readily link the wallet address to the name of an individual. The wallet address contains a user code that serves as a digital signature in the distributed ledger (i.e., a public key) in the form of a unique string of numbers and letters. However, additional information will be necessary to associate the address to a real or natural person.

4.5 Submission of required information

Suspicious Transaction Reports (STRs) filed by obliged entities operating in the VA space or engaging in covered VA activities, such as legal professionals, must be filed, directly or indirectly, depending on the country, to the local FIU. Additionally, FIUs should be able to obtain additional information from reporting entities in their jurisdiction and should have access on a timely basis to the financial, administrative, and law enforcement information that the FIU requires to undertake its functions properly.

It was deemed important during the Seminar that competent authorities should be able to obtain access to all necessary documents and information, including powers to use compulsory measures for the production of records, held by obliged entities. They should have effective mechanisms in place to identify whether natural or legal persons hold or control VA accounts or wallets and mechanisms for ensuring that competent authorities have a process to identify assets, including VAs, without prior notification to the owner.

4.6 Additional best practices dealt with during the face-to-face seminar

During the Seminar, as a result of the practical exercises conducted by the trainers, certain daily best practices were also discussed:

- Generate a commonly used registry of Non-Fungible Tokens (NFTs) with both public (with public access) and private keys (with private access) aligned with owners/users.
- Regarding which evidence of payments with VA, it was advised that such operations are traded via VASP.
- Regarding which evidence should be gathered by legal professionals for real estate (or other) purchases paid for with VA, it was advised that the seller should state the amount, date and address and the legal professional should look for it in the proper blockchain, to verify the payment has been completed.
- In case an individual wants to operate with VA, the best way to ensure a certain address belongs to that individual is to request the individual to operate, in presence of the legal professional, with that address.
- Whenever there is a suspicion on the veracity of an address, the best way to confirm its existence is to google the address.

Conclusions

As a general conclusion, countries have adopted different approaches for regulating legal professionals as obliged subjects to the compliance of the FATF Recommendations and the EU Directives in the legislation regarding AML/CTF, and the level of expertise and compliance also differ among the legal professionals.

Nevertheless, the obligations related to the pillars of ML/TF prevention, namely the due diligence measures (identification of the client 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 obliged entity), the reporting of suspicious transactions and the internal control measures, are the same and should be implemented applying a risk-based approach.

This means that, as a first step, legal professionals must identify, assess and understand their money laundering and terrorist financing risks, develop their policies and procedures to assess risks, apply resources to ensure that they are mitigated effectively and document risk assessments, strategies, policies and procedures to monitor, manage and mitigate ML/TF risks.

Among the member countries, there are some AML/CFT systems in the legal professionals' sector, where the assessment of the sector's risk, the development of the policies and procedures for AML/CFT and the training of legal professionals are the responsibility of the Self-Regulatory Bodies, which guarantees homogeneity and uniformity in the requirements for the application of these policies throughout the 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.

Regarding CDD, some examples of best practices to be conducted are related to the personal identity documents verification in an open database (Ministry of Interior, Consular Section), the verification by bank/insurer/Social, Healthy & Pension Funds, the verification based on certificates and other relevant documents issued by an employer and the verification based on public registers database.

In addition, one of the difficulties in the application of CDD is the identification of the beneficial owner, mainly in the lawyer's sector. In this sense, some examples of best practices when applying CDD measures, agreed during the related seminar, are the extensive exploration of public information stored at the Registry of Beneficial Owner(s) and the exploration of close family, business and political relationships and contacts among potential beneficial ownership(s).

In terms of detection and reporting of suspicious transactions, it is recognized the need for legal professionals as guardians of legality in countering anti-money laundering and terrorist financing phenomena. While believing that automated reports based on the most sophisticated artificial intelligence tools are important, it emerged that the

presence of highly qualified professionals who intercept transactions at their genesis and who know how to detect the presence of dangerous indexes as soon as possible is essential.

Thus, there was a common feeling and wish for constant training in AML/CFT, and how the ideal professional regarding AML/CFT, is that of an independent, authoritative person who has a loyal collaborative role with public authorities.

In doing so, as guarantee of such professionality, the Seminars proved that it is essential to have access to a clear and detailed list of indicators and red flags for legal professionals that help detect suspicious transactions.

In some of the member countries, the legal professionals' sector have implemented systems for the prevention of money laundering and terrorist financing where the development of risk indicators and red flags to facilitate the detection of suspicious transactions as well as the analysis of suspicious transactions submitted by the legal professionals and the report to the competent authorities are the responsibility of AML/CFT specialists integrated in the Self-Regulatory Body, which guarantees professionals with experience in AML/CFT are responsible for conducting the analysis.

This practice has also demonstrated its effectiveness in the level of compliance with the reporting obligations in the sector, and therefore the inclusion of AML/CFT specialists, independent but within the Self-Regulatory Bodies, is also highly recommended.

In addition, regarding the best practices to mitigate the risks related to the use of VA, the CCD of the legal professionals must focus on the identification of the beneficiary of the operation, as well as on establishing the legitimate origin of the funds. Notaries/lawyers should ask their customer to prove the ownership of the funds, and do, when possible, some verification of the information provided by their customers.

In relation to the existence of the funds in VA, if they are located at a certain address provided by the client, it can be verified by consulting the blockchain. However, if the funds are in a centralized Virtual Assets Service Provider (VASP) that correctly applies CDD, it could be possible to request some type of certificate from that company on the existing balance in the client's account.

In relation to the funds belonging to the client, and if the funds are deposited in these reliable VASPs, a legal professional could also request some type of certificate to that VASP regarding the owner of these funds.

In case that the funds are deposited in non-hosted wallets, the mere possession of the private key only indicates that the person who possesses it really has access to the funds, and this case could be assimilated to the person who presented a large amount of cash to carry out the operation. However, on contrary to that analogy, another person from elsewhere could also access the funds if he had a copy of that private key.

Regarding which evidence should be gathered by legal professionals for real estate (or other) purchases paid for with VA, it was advised that the seller should state the amount,

date and address and the legal professional should look for it in the proper blockchain to verify the payment has been completed.

In summary, the best practices identified are intended to raise awareness in the legal professionals about their vulnerabilities and risk exposure to ML/TF and to improve the compliance level with AML/CFT obligations in these sectors, mainly related to the framework to prevent ML/FT, the identification of individuals/entities and their ultimate beneficial owners, the detection, analysis and reporting of suspicious transactions, and the new threats inherent to virtual assets.

To this end, it is also essential to promote the continuous training of legal professionals, as well as their continuous updating on new trends and typologies related to these crimes.