HANDBOOK FOR THE APPLICATION OF MEASURES FOR PREVENTING AND COMBATING MONEY LAUNDERING AND TERRORIST FINANCING BY DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

Chisinau, 2018

OFFICE FOR PREVENTION AND FIGHT AGAINST MONEY LAUNDERING

The Office for Prevention and Fight against Money Laundering (hereinafter the OPFML) is a public law authority within the Government of the Republic of Moldova, which functions as an autonomous and independent specialized central body. The Office's activity is geared towards preventing and combating money laundering and terrorist financing, and contributes to ensuring the state security.

For more details on the OPFML, please, visit the official website of the institution:
www.spcsb.md

The handbook has been developed with inputs from the EU/CoE project on Controlling Corruption through Law Enforcement and Prevention (CLEP).

Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe

TABLE OF CONTENTS

FOREWORD

This Handbook for the application of measures for preventing and combating money laundering and terrorist financing by Designated Non-Financial Businesses and Professions (DNFBPs) (hereinafter "the Handbook") has been developed by the Office for Prevention and Fight against Money Laundering of the Republic of Moldova (hereinafter OPFML or the Office), with inputs from the CoE/EU Project on Controlling Corruption through Law Enforcement and Prevention (CLEP).

The Handbook provides a description of the application of measures for preventing and combating money laundering and terrorist financing by lawyers, notaries, accountants, auditors, casinos and other gambling service providers, dealers in precious metals and/or precious stones, real estate agents and others (hereinafter: DNFBPs[1] or reporting entities).

The Handbook has been designed for and targets resident and non-resident physical and legal persons that carry out their activities in the Republic of Moldova, as well as representation offices/branches of foreign companies registered in the Republic of Moldova, whose main activity is provision of services in the fields referred to above. The objective of the Handbook is to facilitate enforcement and implementation of the Law No. 308 of 22 December 2017 ‚On Prevention and Combating of Money Laundering and Terrorism Financing' by reporting entities as subjects of the supervisory regime.

In order to keep this work consistent and clear, the terms used herein correspond to the concepts used in **Law No. 308 of 22 December 2017 ‚On Prevention and Combating of Money Laundering and Terrorism Financing'** (hereafter referred to as the Law 308/2017). Increase the understanding of the relevant national and international legislation by reporting entities and other stakeholders will limit the uncertainties associated with the legal and institutional requirements.

The national legal framework on the application of measures for preventing and combating money laundering and terrorist financing for the reporting entities is established, although not limited to the following sources:

a. Law No. 308 of 22 December 2017, On Prevention and Combating of Money Laundering and Terrorism Financing';
b. Instruction on the application of the international restrictive measures approved by Order of the OPFML Director No. zz of zz.zz.2018;
c. Guide on the identification and monitoring of beneficial owners approved by Order of the OPFML Director No. zz of zz.zz.2018;
d. Instruction on reporting of activities or transactions falling within the scope of Law No. 308 of 22 December 2017 ‚On Prevention and Combating of Money Laundering and Terrorism Financing' approved by Order of the OPFML Director No. 18 of 08 June 2018;

[1] As defined under article 3 of law No. 308 of 22 December 2017 on prevention and combating money laundering and terrorism financing, the DNFBPs are natural or legal persons that provide independent professional accounting, audit, and legal nature services, including lawyers, notaries, acting in accordance with the legislation in force;

e. Guidelines on the identification and monitoring of politically exposed persons, approved by Order of the OPFML Director No. 17 of 08 June 2018;

f. Guidelines on identification of terrorist financing suspicious activities and transactions, approved by Order of the OPFML Director No. 16 of 08 June 2018;

g. Guidelines on identification of money-laundering suspicious activities and transactions, approved by Order of the OPFML Director No. 15 of 08 June 2018;

h. Methodology on identification of money laundering and terrorist financing suspicious activities and transactions, approved by Government Decision No. 496 of 25 May 2018;

i. Orders of the Director of the Intelligence and Security Service on consolidated lists of persons, groups and entities involved in terrorist activities;

l. Action Plan on the Reduction of Risks in the Field of Money Laundering and Terrorist Financing 2017-2019, approved by Government Decision No. 791 of 11 October 2017.

With regards to international instruments, the following shall be taken into consideration:

a) EU Directive 2015/849 of 20.05.2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing.

b) Recommendations of the Financial Action Task Force (FATF-GAFI).

c) Unanimously recognized rules of international law, international treaties to which the Republic of Moldova is a party, and other normative acts regulating relations in this field.

The sources above are available on the official website of the OPFML: www.spcsb.md, as well as in other documents and guidelienes published by the FATF[2].

The ***Handbook for the application of measures for preventing and combating money laundering and terrorist financing by Designated Non-Financial Businesses and Professions*** has been developed with the aim to provide a practical useful tool in fulfilling specific legal obligations. The Handbook contains useful information systematized on the basis of the national laws and international standards, as well as under secondary normative acts approved in the field of prevention and combating of money laundering and terrorist financing. The Handbook also presents various money laundering typologies and practical examples that describe the methods used by different subjects in the money laundering process, based from the experience of Moldova and other countries.

OPFML relies on the significant contribution and commitment of the reporting entities in implementing their legal obligations and it offers the Handbook to this end.

[2] Financial Task Force:

- ✓ Money Laundering and Terrorist Financing Vulnerabilities of Legal Professions,June 2013;
- ✓ Money Laundering and Terrorist Financing through the Real Estate Sector, June 2007;
- ✓ RBA Guidance on casinos, October 2008;
- ✓ Vulnerabilities of casinos and gaming sector, March 2009;
- ✓ RBA Guidance for accountants, June 2008;

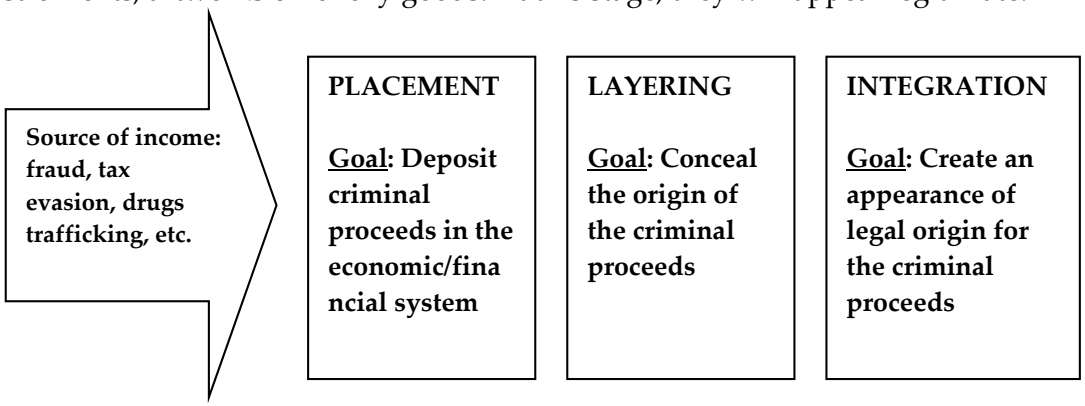
INTRODUCTION

1) What is money-laundering?

1. **Money laundering (ML)** is not a new phenomenon, on the contrary it is deeply rooted in the past, with "a corrosive effect on a country's economy, government and social well-being". It implies concealing the origin of criminal assets to give the appearance of lawfulness to some goods The term of **money laundering** was used during the 1920s in the United States of America, being associated with members of organized crime groups. The use of the term focused on the feature of disguising the origin of funds through different business, such as car washes and laundries to justify the origin of proceeds from various criminal activities.
2. Internationally, the issue of money laundering was addressed by the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, adopted on 20 December 1988 in Vienna. The parties to the Convention sought to raise awareness of the international community on the fight against illicit traffic in narcotics, which is a source of revenues that enable criminal organizations to corrupt state structures, commercial and financial businesses and, ultimately, the society at all its levels.
3. Disguising the origin of illicit goods or assets may involve not only financial and banking institutions, but also representatives of DNFBPs, such as lawyers, notaries, accountants, auditors, luxury goods dealers, real estate agents, gambling service providers and dealers in precious stones and metals.
4. The Financial Action Task Force (FATF) is an international organization that sets standards on preventing and combating money laundering and financing of terrorism and defines the term of money laundering as "the processing of criminal proceeds to disguise their illegal origin".
5. **The Criminal Code of the Republic of Moldova** defines money laundering as follows (article 243):
   a) Conversion or transfer of goods by a person who knows or ought to have known that such goods are illicit income, for the purpose of concealing or disguising the illicit origin of the goods, of assisting any person who is involved in the commission of the main offense, or of evading the legal consequences of these actions;
   b) Concealment or disguise of the nature, origin, location, disposal of, transfer, movement of real estate or related rights by a person who knows or ought to have known that such property is illicit income;
   c) Acquisition, possession or use of goods by a person who knows or ought to have known that such goods are illicit income;
   d) Participation in any association, arrangement, complicity by assisting, facilitating or counselling the commission of the above-mentioned actions.
6. There are three stages in money laundering: **placement, layering and integration.**
   a) **Placement:** The first stage of this process includes the placement of money from illegal sources in the legal economic/financial system, usually through a financial institution. This can be carried out, for example, by opening a deposit account using cash. Large amounts are divided into several smaller amounts so as not to attract attention, and then they are gradually deposited with different branches of the same bank or with different banks. Currency exchanges or conversion of small denomination banknotes into large denomination banknotes can be done at this stage.
   b) **Layering**. The second stage of money laundering begins once the placement is finalized, and implies a series of transfers or movements of money, securities and other assets to other institutions or other beneficiaries in order to disguise and camouflage the illegal original

source. Such funds may be used to acquire other liquid or semi-liquid assets, which in turn will be sold or transferred to other beneficiaries. Money laundering can also be carried out through a payment transfer for some goods or services, or by transferring funds to the accounts of a shell company or an intermediary entity.

c) **Integration.** The third stage consists of making the funds and goods available as part of the legal system. This is possible by obtaining assets such as real estate, financial or monetary instruments, artworks or luxury goods. At this stage, they will appear legitimate.



7. Three stages are also used in terrorist financing procedures: fund raising/collection, transfer and distribution. **Art. 279 of the Criminal Code of the Republic of Moldova defines** terrorist financing as deliberate provision or collection by any person, by any means, directly or indirectly, of any kind of goods acquired by any means, or provision of financial services with the purpose of using these goods or services or knowing that they will be used in whole or in part:

a) To organize, prepare or commit a terrorist offense;

b) For any purpose, by an organized criminal group, a criminal organization or a particular person committing or attempting to commit a terrorist offense, or organizing, directing, joining, pre-arranging, instigating or participating as an accomplice in committing this crime.

8. Whatever the level of development of the countries in question, money laundering and terrorist financing are activities that compromise social stability, internal security, transparency and the efficient and effective functioning of public and private institutions. Fundamentally, money laundering and terrorist financing are simple concepts. If money laundering is a process whereby proceeds from illicit activities are transformed so as to be disassociated from their illegal origin, terrorist financing is a financial and material support, in any form whatsoever, of terrorism or of those who encourage it or engage in it.

9. Money laundering and terrorist financing are carried out by means of similar transactions and activities, most of which are related to concealment of goods. Money launderers convey illicit goods through legal channels to conceal their criminal origin, while those who finance terrorism transfer assets, which may be legal or illegal, using a way to conceal the source and the purpose of their use, thereby supporting terrorism. The techniques used to launder money are essentially the same as those used to conceal the source or the purpose of financing terrorism.

10. If the source can be concealed, it remains available for future financing of terrorist activities. It is equally important for terrorists as for criminal involved in money laundering to conceal the use of funds so that their financing remains unidentified.

11. Material support to terrorist organizations may derive from legal activities as well (for example donations, sales, commercial actions), and when the goods deriving from an illegal

activity are mixed, they are particularly difficult to be identified among legal goods that support terrorist organizations. In order to remain disguised, terrorist organizations need to use apparently assets with legal appearance. Once the goods originating from offenses have been converted into legal assets, they can be entrusted (a frequent process) to terrorist organizations to be used for their criminal purposes.

12. Terrorist groups are not interested in making profits, but only in obtaining sources able to finance their actions, so illegally or legally obtained goods are often found in very small amounts, and they are hardly identified as terrorist financing acts. In the case of transactions that took place before the attacks of September 11, 2001, individual transactions did not reach ten thousand dollars and were made through simple transfers, allegedly by students who seemed to receive money as state scholarships or from parents' funds.

13. *Fund raising/collection* involves three main sources:

a) Illicit sources (often connected to organized crime);
b) Licit sources (for instance, donations, gifts from legal sources, etc.);
c) Providing logistical support (such as accommodation, transport, training, etc.) as a complex form of insurance, with or without visible costs of the necessary support for terrorist activities in which both legal and illegal sources can be used. Material support is not classified in all cases as TF.

14. In the Republic of Moldova, the terrorist issue is addressed focusing on prevention, which implies paying more attention to supplying terrorist activities with human, logistical and financial resources. Consequently, the institutions empowered to prevent and combat terrorism actively engage, depending on their competences, in activities aimed at stopping financing of terrorist groups, while cooperating with the Office in identifying terrorist financing suspicious transactions.

CHAPTER I. AUTHORITIES SUPERVISING THE REPORTING ENTITIES

1) Supervisory authorities

15. Regulation, supervision and control of the enforcement of the laws on prevention and combating of money laundering and terrorist financing in the Republic of Moldova by the non-financial reporting entities is ensured by the following supervisory authorities3:

a) Bar Association of the Republic of Moldova – for lawyers;
b) Notaries Chamber – for notaries;
c) Ministry of Finance – for auditors, audit entities, legal entities and individual enterprises providing accounting services, as well as casinos and other gambling service providers;
d) Assay Office – for natural and legal persons engaged in entrepreneurial activity with precious metals, items of precious metals and/or precious stones (hereinafter, dealers in precious metals and stones);
e) Office for Prevention and Fight against Money Laundering (OPFML) – for real estate agents, as well as dealers in luxury goods (especially for goods with a value above 200,000 MDL).

16. In order to ensure enforcement of the provisions of the Law on prevention and combating of money laundering and terrorist financing and of the relevant international standards, the authorities supervising the reporting entities, subject to their competencies:

a) Issue orders, decisions, instructions and other normative acts in the field of prevention and combating of money laundering and terrorist financing, in the cases provided for by Law No. 308 of 22 December 2017;
b) Approve and publish guidelines and recommendations necessary for the supervised reporting entities to implement provisions of Law No. 308 of 22 December 2017;
c) Monitor and verify application of provisions of the present law, of the normative acts subordinated to it, of relevant programs of the reporting entities and of the instructions regarding the application of the customer due diligence measures, customer identification and beneficial owner, reporting, storage of data on performed activities and transactions, as well as on the execution of the internal control measures and procedures.

17. Under the Law on prevention and combating of money laundering and terrorist financing, the supervisory authorities have the following obligations:

a) To determine whether the reporting entities use written policies, methods, practices and procedures as well as internal control measures and whether the reporting entities comply with their own programs aimed at preventing and, where appropriate, identifying money laundering and terrorist financing activities;
b) To inform the reporting entities about money laundering and terrorist financing transactions, including about new methods and trends in this area;
c) To identify whether the reporting entities have possibilities to launder money and finance terrorism, to take additional measures, where necessary, to prevent illegal use of their professions and to inform the reporting entities of any risks;
d) To notify the other supervisory bodies of the reporting entities about the identified violations in the area of money laundering and terrorist financing, for measures to be taken to withdraw authorizations for entrepreneurial activity.

18. In order to ensure effective cooperation in the field of prevention and combating of money laundering and terrorist financing, the supervisory authorities are under the obligation to

[3] Find more details about supervising authorities in the field of prevention and combating of money laundering and terrorist financing in Art. 15 of Law No. 308 of 22 December 2017.

notify the Office for Prevention and Fight against Money Laundering within at least 24 hours if during their inspections carried out at the reporting entities or by any other means, they have identified facts that may be related to money laundering or terrorist financing.

2) The Office for Prevention and Fight against Money Laundering.

19. OPFML is an independent public authority in relation to the other legal and physical persons, irrespective of the type of ownership and legal form of organization, and it functions as an autonomous and independent central specialized body, empowered to prevent and combat money laundering and terrorist financing[4].

20. The OPFML also has free online access to information resources, including those containing personal data, created and maintained by public authorities and supervisory bodies.

21. The OPFML examines information on suspicious activities and transactions which may be linked to money laundering or terrorist financing originating from sources other than those obtained from competent authorities, supervising authorities or reporting entities, including based on its own initiative.

22. The OPFML has also the right to ask the reporting entities to apply due diligence measures depending on the risk associated with certain customers, products, services, jurisdictions and business relationships, as well as to apply injunctive relief.

23. The OPFML may require the competent bodies to carry out within their competence inspections aimed at establishing the economic meaning of the operations, the nature of the business relationship, the source of the goods, the beneficial ownership and the observance of the tax regime.

24. The OPFML has the right to request and receive, within the deadline specified in the requests, the following types of information from reporting entities:

a) Necessary information and documents available to the reporting entities, their customers and the public administration authorities, in order to determine the suspicious nature of the activities or transactions;

b) Information held by the reporting entities on the monitoring of complex and unusual activities and transactions, customer due diligence, beneficial owners and business relationships;

c) Information from resident and non-resident natural and legal persons on transactions and activities under preparation or carried out;

d) Explanations from natural and legal persons regarding the business relationships and the source of the goods involved in suspicious activities and transactions which may be linked to money laundering, related offenses and financing of terrorism;

e) Documents related to customer due diligence measures and internal control;

f) Relevant information on the outcome of examination of notices in accordance with the provisions of the Law No. 308.

More details on how the Office operates and on its achievements may be found in its annual reports, published on the official website: www.spcsb.gov.md/acivitate.

[4] The distinct duties and functions of the OPFML are expressly provided for in Art. 19 of Law 308/2017.

CHAPTER II. RISK-BASED APPROACH (RBA)

25. The Risk-Based Approach (RBA) means that countries, competent authorities, and banks/DNFBPs identify, assess, and understand the money laundering and terrorist financing risk to which they are exposed, and take the appropriate mitigation measures in accordance with the level of risk.

26. According to the provisions of Art. 6 para. (2) and (3) of Law 308/2017, the reporting entities apply the risk-based approach individually, in order to determine the extent of the vulnerabilities and of the money laundering and terrorist financing risks. The application of this legal provision allows for measures to prevent or mitigate the phenomenon of money laundering and terrorist financing, which are proportionate to the identified risks. This requirement will also facilitate the allocation of resources to the reporting entities in the most efficient way, so that they are used in line with the reporting entity's priorities of identifying the main risks and vulnerabilities.

27. Irrespective of the power and effectiveness of the control systems for preventing and combating money laundering and terrorist financing, offenders will continue their attempts to transfer funds and illicit goods without being detected, and in some cases they will succeed. Offenders are more likely to use the reporting entities referred to in this Handbook if other ways of money laundering or terrorist financing become more difficult. For this reason, the reporting entities may be more or less vulnerable, depending on how effective procedures for preventing and combating money laundering and terrorist financing are. A risk-based approach allows the reporting entities to adapt themselves more effectively to detected vulnerabilities as new money laundering and terrorist financing methods are identified.

CHAPTER III. ASSESSMENT OF MONEY LAUNDERING RISK AND TERRORIST FINANCING RISKS AT NATIONAL LEVEL

28. One of the international obligations of the Republic of Moldova is to undertake a National Risk Assessment (NRA) on prevention and combating of money laundering and terrorist financing Thus, the key objective of the NRA is to identify, analyse and recognize the money laundering and terrorist financing risks faced by the Republic of Moldova. In fact, identifying the nature and impact of the national risks will certainly influence the determination of the level of control measures applied to a particular product or sector.

29. The Office, jointly with other supervisory bodies and law enforcement bodies, are responsible for organizing the NRA on money laundering and terrorist financing, which is run at least once every 3 years. The NRA aims at optimizing the AML/CFT normative and institutional framework, contributes to the efficient distribution of resources at all levels of the regime for prevention of money laundering and terrorist financing, which includes the Office, the supervisory authorities, the law enforcement bodies, the reporting entities and other competent institutions.

30. The NRA report also outlines the results of the assessment in the fields concerning DNFBPs as reporting entities. For this reason, it shall be used by the reporting entities as a reference to start the continuous process of assessing and identifying risks in a specific sector.

The NRA has rated the money laundering vulnerabilities for the DNFBP sector as follows:

DNFBP type	Vulnerability
Real estate agents	Medium-High
Dealers in precious metals and stones	Medium
Notaries	Medium
Gambling establishments	Medium
Lawyers	Low
Accountants and auditors	Low

More specifically, with regard to the real estate sector, the NRA underlines the issues of use of cash in real estate-related transaction and the failure to identify and report suspicious transactions. Similar issues affect the vulnerability of dealers in precious metals and stones.

While the notaries have reported suspicious transactions in the past, the level of reporting is still low. Similar issues have been identified for lawyers. More specifically for the notaries the NRA also notes the decreasing value of authenticated contracts compared to the declared cadastral value, which may be used to avoid taxes.

Gambling establishments also require better control of due diligence and suspicious transaction reporting whereas for accountants and auditors, a more proactive role of the supervisory body is seen as a need in the NRA, coupled with more training especially on risk typologies.

For all DNFBPs, the NRA notes the following issues:

- ✓ Lack effective implementation of supervision of compliance with AML requirements;
- ✓ Gaps in the identification of PEPs and beneficial owners;
- ✓ Lack of specific provisions requiring establishing the origin of funds in intermediary transactions, particularly significant considering that Moldova is a cash-based economy.

CHAPTER IV. RISK ASSESSMENT IN RESPECTIVE FIELDS OF ACTIVITY

31. Taking into account the NRA on money laundering and terrorist financing described in Chapter III of this Handbook, the reporting entities will undertake actions to identify and assess money laundering and terrorist financing risks in their own activities (not at the sectorial level), using for this purpose criteria and factors established by the supervisory bodies.

32. In order to ensure an adequate assessment process of the risks in each field of activity, the reporting entities use different variables specifically related to the nature of the business. This relates to the destination of a good or of a business relationship, the amount of assets or of transactions carried out by the customer, the frequency and duration of the business relationship.

33. According to Art. 6 of Law 308/2017, the reporting entities are obliged to identify and assess the money laundering and terrorist financing risks in their own field of activity before:

a) Launching and developing new products and services;
b) Using new or emerging technologies, for both new and existing products and services.

34. The reporting entities will assess the risks by determining their scale according to the following aspects:

a) Customer;
b) General risk of money laundering and terrorist financing identified;
c) Country (jurisdiction) involved;
d) Business relationship;
e) Good, service or transaction, and their channel of delivery.

35. Depending on the size and nature of the activity, the reporting entities may identify other factors or sources of risk that will complement the risk assessment of money laundering and terrorist financing in their respective field of activity.

36. The risk analysis shall be conducted in such a way as to identify the directions where the money laundering and terrorist financing risks are the highest. The reporting entities shall identify the main vulnerabilities and minimize them appropriately through preventative measures. The reporting entities will use this information to identify major-risk customers and services and high-risk geographic areas. It is essential to understand that these assessments are not static in nature. On the contrary, they should change over time depending on how the circumstances and threats of money laundering and terrorist financing will evolve.

CHAPTER V. APPLICATION OF CUSTOMER DUE DILIGENCE MEASURES

1) Due diligence

37. Customer Due Diligence (CDD) is a set of actions aimed at obtaining specific information from customers. Such information enables the reporting entity to estimate and assess how a particular customer is exposed to money laundering and terrorist financing risks and take measures commensurate to the level of risk identified. Client identification records shall be kept. There is a difference between natural and legal persons. In case the customer is not a natural person, legal status of the customer shall be confirmed with appropriate documents, including his/her authorization to act.

38. CDD measures are applied by the reporting entities to both new and existing customers. Thus, the reporting entities will apply the following CDD measures:

a) Identification and verification of the identity of customers based on identity documents as well as documents, data or information obtained from a reliable and independent source;
b) Identification of the beneficial owner and adoption of appropriate risk-based measures to verify his/her identity. The reporting entity shall confirm the identity of the beneficial owner, including by adopting reasonable measures to understand the ownership and control structure of the legal person;
c) Understanding and, if necessary, obtaining and assessing the information on the purpose and desirable nature of the business relationship;
d) continuous monitoring of the business relationship, including examination of transactions concluded throughout the relationship concerned, to ensure that the transactions made are consistent with the information held by the reporting entities on the customer, the profile of his/her activity and risk, including the source of the goods, and that the documents, data or information held are up to date.

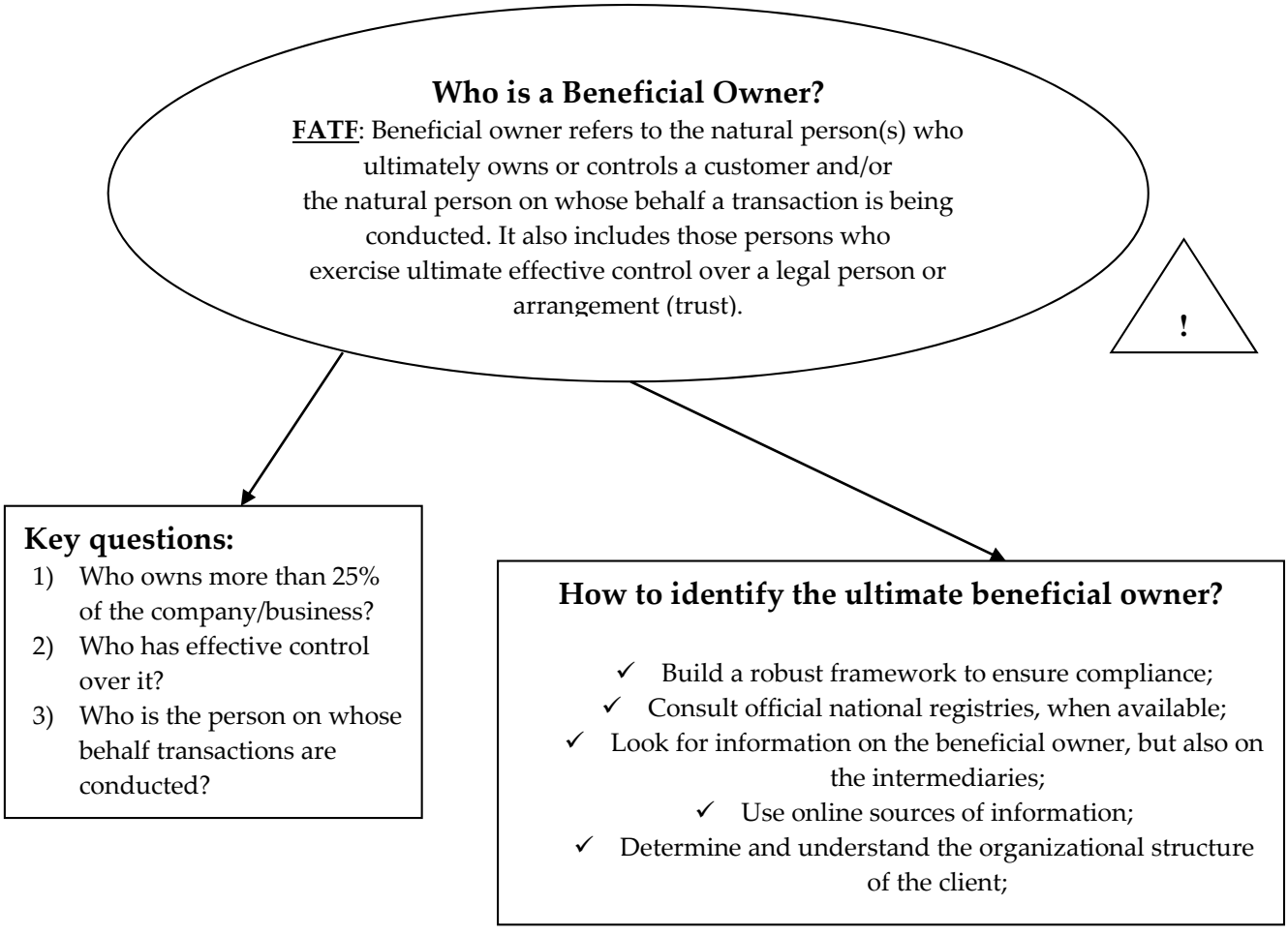
39. For the purpose of implementing the provisions of related AML/CFT laws, the reporting entities apply the CDD measures:

a) Before the business relationship is initiated;
b) In the course of all types of occasional transactions: worth more than 300,000 MDL if carried out through one or several transactions connected to each other, having due regard to the national requirements;
c) When there is a suspicion of money laundering or terrorist financing, regardless of deviations, exemptions or established limits;
d) When truthfulness, sufficiency and accuracy of previously obtained identification data is doubtful.

40. If it is not possible to comply with the requirements of point (48) let. (a)-(c) of this Handbook (e.g. failure to obtain other relevant documentation), the reporting entities shall not engage in any transaction or activity, including not to establish a business relationship or terminate an existing business relationship. In addition, they are encouraged to consider submitting forms on suspicious transactions or activities to the Office. In this case, the reporting entities are entitled not to explain to the customer the reason of the refusal.

CHAPTER VI. BENEFICIAL OWNERSHIP, TIPS FOR EFFECTIVENESS IMPLEMENTATION

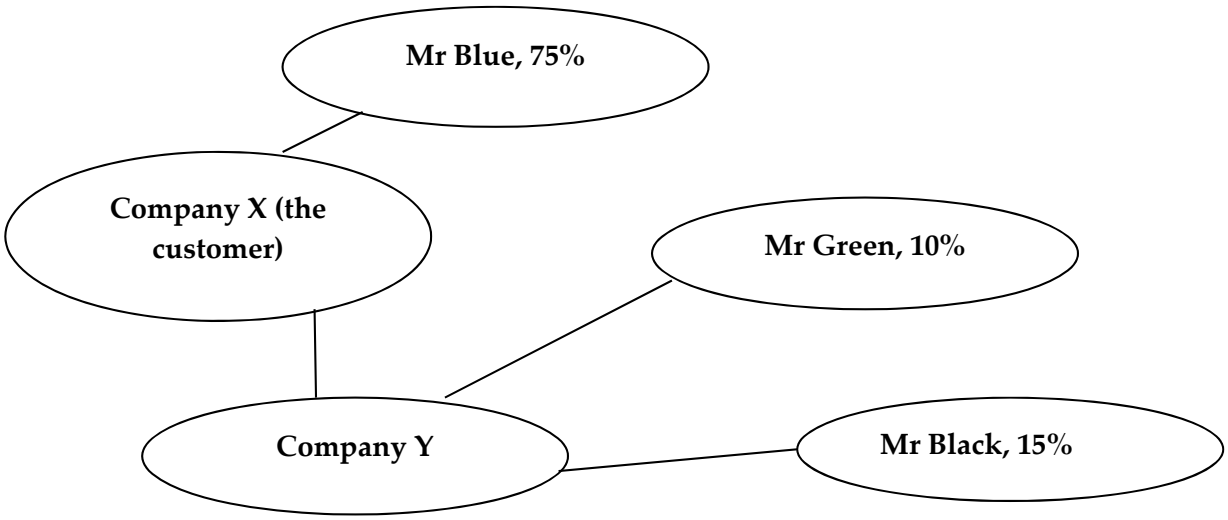
41. Reporting entities should pay particular attention to the requirements concerning beneficial owners. In most cases, your client (natural person) will be the same person in whose name or interest a transaction will be conducted or a service requested. However there could be cases, for example, when a customer is a legal entity or a foreign trust, or if a customer is acting in the interest of someone else, in which case the reporting entity will have to establish who the beneficial owner is, and then identify and verify that person. There have been many money laundering cases in which legal entities, trust or individuals acting as a "front" for someone else were used to hide the money trail and the illicit origin of the proceeds. Who is the beneficial owner, and how can a reporting entity establish who is the beneficial owner? As shown below the FATF definition of beneficial owner, which was incorporated in the anti-money laundering Law of the Republic of Moldova, emphasizes two key concepts: 1) ***Ultimate ownership*** and 2) ***Ultimate effective control*** over a customer (be it a natural person, a legal person or a legal arrangement, such as a trust)[5]:



An example: Company X is owned by Mr Blue, who owns 75% of the shares, and is equally owned by two other individual, Mr Green and Mr Black. Assuming this ownership structure is correct,

[5] Financial Action Task Force, 2014, Transparency and beneficial ownership, accessed in December 2018;

the identity of the individuals owning more than 25% of the shares of the companies shall be clarified.



42. Establishing who the beneficial owner is, will vary depending on the types of customers. For example, when it comes to "control" in a company limited by shares, two groups of people might arguably qualify as having ultimate control: 1) the shareholders (in the scheme above); but also 2) the board of directors.

43. A research conducted by the World Bank[6] on the use of legal entities in corruption cases has shown that in identifying the beneficial owner, the focus should be on two factors: the ***control exercised*** and the ***benefit derived***. The scheme above provides for an example of control through ownership. However control of a legal entity will always depend on the context, as control can be exercised in many different ways, including through ownership, contractually or informally. A formal approach to beneficial ownership, based on percentage thresholds of ownership or designated beneficiary of a legal person, such as in the scheme above, may yield useful information providing clues to the company's ultimate ownership or control. More generally, it may lead to the identification of people of interest who possess information regarding the beneficial owners. Other persons may also be relevant to establish who the beneficial owner is: for example, the person having delegated signatory authority by the legal representative of the legal person (who may not be a shareholder or a director) could qualify as the beneficial owner.

44. Reporting entities should be aware of the risk of concealing beneficial ownership particularly when dealing with "shell" companies, namely a non-operational company that has no independent operations, significant assets, ongoing business activities, or employees, particularly if established in an offshore financial centre.

45. Reporting entities should also be aware of the peculiarities related to beneficial ownership if and when dealing with trusts. "Trusts" cannot be created under Moldovan law, but they can be created in other jurisdictions, and their use is not infrequent, including in countries of the former Soviet Union, for hiding beneficial ownership. In a typical trust, a grantor or settlor transfers the legal title to property (the right to control the property) to a trustee, and the

[6] World Bank and United Nations Office for Drugs and Crime, Stolen Asset Recovery Initiative, 2011, The Puppet Masters, How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It, accessed in December 2018;

equitable title (the right to enjoy the benefits of the property) to beneficiaries. As explained in the World Bank research mentioned above, in the case of a trust several people could qualify as the beneficial owner:

• The *trustee* because he/she conducts the day-to-day management of the asset held in trust and could—if he/she wanted—dispose of it in any way. He/she is, however, legally bound to act in the interest of the beneficiary as set out in the deed of trust. Therefore, the trustee is not an ultimate controller but rather acts *on behalf of* someone else and is under fiduciary obligations.

• The *settlor*, because he/she initiated the trust and contributed the asset to the trust in the first place. The settlor, however, is no longer able to exercise control over the trust.

• The *beneficiary*, because he/she stands to benefit. However, the beneficiary similarly cannot exercise control over the trust.

46. For trusts, the control of the assets and their ownership is split. Normally a trustee controls the trust (but does not benefit from it); and a beneficiary has no control over the trust but has the right to benefit from it (and ultimately has ownership of the assets). This means that for a trust or other legal arrangements, it is not enough to only identify a single controlling owner but that the trustee and the beneficiary should be identified, and also the settlor and the protector[7] (if there is one).

47. The FATF and the Egmont Group have published a research on concealment of beneficial ownership[8] and noted that, when considering the beneficial ownership of a trust, asking the following key questions may assist reporting entities to better understand key features of the arrangement:

1. Who is the real settlor and what is the real source of funds?
2. Who are the real beneficiaries i.e. for whose benefit are the trust assets managed?
3. What is the trust's governance system and who are the real "natural persons exercising effective control"?

48. A source of information for establishing who the beneficial owner of a trust is to ask the trustee a copy of the trust deed or regulations, showing the beneficiaries or the explanation of the purpose of the formation of the trust.

Below is a real case example[9] of the use of trusts in ML schemes:

Trust established to receive proceeds of tax crime and invest in criminal property

Two trusts were established in an offshore centre by a law firm. The law firm requested the trustee to accept two payment orders in favour of a bank in order to buy real estate. It appeared that the trust had been used to conceal the identity of the beneficial owners.

Information obtained by the Belgian Financial Intelligence Unit revealed that the beneficiaries of the trusts were individuals A and B, who were managers of two companies, established in Belgium. Both were the subject of a judicial investigation regarding serious tax fraud and part of the funds in these trusts could have originated from criminal activity of the companies.

Simplified due diligence

49. The reporting entities may apply simplified CDD measures to their customers if, by their nature, they or representatives thereof may present a low money laundering or terrorist financing risk. It is very important to underline that simplified CDD measures in no way can

[7] The protector is typically entrusted by the settlor with the responsibility to ensure that the trustees act in the interest of the beneficiary established by the deed creating the trust.

[8] Financial Action Task Force, 2018, *Concealment of beneficial ownership*, accessed in December 2018;

[9] *Ibidem*

be applicable if there is a suspicion of money laundering or terrorist financing with respect to the customer or its transaction. Furthermore, simplified CDD shall not be allowed in high-risk circumstances as identified by the Moldovan authorities through the NRA process or by sectorial supervisors. The circumstances of application of simplified CDD shall remain limited. Know-Your-Customer information shall still be obtained.

50. Simplified CDD measures will include the following actions:

a) Verification of identity of the customer and of the beneficial owner after establishing the business relationship;
b) Reduced the frequency of updating of identification data;
c) Reduced level of continuous transaction monitoring or of the business relationship;
d) Less detailed information to be gathered about the purpose and nature of the business relationship.

51. Based on its own assessment and reasoning, the reporting entity shall set out factors that generate low risks of money laundering and terrorist financing, which may lead to simplified CDD. For example, simplified CDD could be applied when the customer is a company whose securities are traded on a regulated market/in a multilateral trading system requiring proper transparency of beneficial owner, or when the customer is well known by the reporting entity because of a long-standing business relationship.

52. During their activity, the reporting entities may encounter complex and unusual activities or transactions as well as lack of clear legal or economic purpose. If, following an assessment, it is concluded that there is a high risk of money laundering or terrorist financing, the reporting entities are required to apply enhanced CDD measures. These measures shall be commensurate to the identified risks. In order to minimize potential risks, the reporting entity shall enhance monitoring of the business relationship to determine whether transactions or activities performed are suspicious or unusual.

53. The reporting entities shall apply enhanced CDD measures when customers' activities or transactions present an increased risk of money laundering or terrorist financing, as well as in other situations, according to criteria and factors set by the supervisory bodies, including:

a) Obtaining additional information on the customer (type of activity, volume of assets, turnover, other available information in public sources including on the Internet) as well as frequent updating of the identification data of the customer and the beneficial owner;
b) Obtaining additional information about the nature and purpose of the business relationship;
c) Obtaining information about the source of the customer's goods;
d) Obtaining information about the purpose of the transaction or the activity under preparation, about to be performed or already performed;
e) Obtaining the approval from the person with senior management functions for initiation or continuation of the business relationship;
f) Enhanced monitoring of the business relationship by increasing the number and extending the duration of verifications carried out and by selecting transactions and activities requiring an additional examination;
g) Requesting that the first payment of transactions is made through an account opened on behalf of the customer with a financial institution, which applies similar CDD measures.

54. On the basis of its own assessment, the reporting entity sets out the factors that generate increased risks and need enhanced customer due diligence measures to be applied. The reporting entities may use the following criteria to decide whether certain factors generate additional risks:

a) Business relationships in unusual circumstances such as long geographical distance between the reporting entity and the customer;
b) Customers residing in jurisdictions with high risk of money laundering and terrorist financing;
c) Customers who do not appear personally for identification;
d) Legal entities with the role to manager personal property management;
e) Companies that have authorized shareholders or whose shares are held in trust;
f) Activities frequently involving cash in considerable amounts;
g) Situations in which the ownership and control structure of the legal person is unusual or too complex, having regard to the nature of its activity;
h) Banking services provided to a natural person on the basis of a customized portfolio negotiated with the customer;
i) Products or transactions able to provide anonymity;
j) Business relationships or remote transactions, without certain protection measures, such as electronic signature;
k) Payments received from unknown or unrelated third parties;
l) New products and new business practices, including new mechanisms for the distribution and use of new or emerging technologies for both new and pre-existing products.
m) Countries of destination which, according to some reliable sources (mutual assessments, published detailed assessment reports or monitoring reports) do not have effective systems in place to prevent and combat money laundering and terrorist financing;
n) Destination countries which, according to some reliable sources, are affected by a high level of corruption or other criminal activities;
o) Destination countries subject to sanctions, embargoes or similar measures, imposed by the relevant international organizations, in accordance with the commitments assumed by the Republic of Moldova;
p) Destination countries that provide funding or support for terrorist activities or on the territory of which designated terrorist organizations operate;
q) Other factors identified within the assessment.

55. The enhanced CDD measures will be applied in business relationships with the involvement of politically exposed persons, members of their families and persons associated with politically exposed persons. Thus, besides the due diligence measures, the reporting entity undertakes the following actions:
a) Develops and puts in place appropriate risk management systems, including procedures based on risk assessment, to find out whether a customer, a potential customer or a beneficial owner of a customer is a person politically exposed;
b) Obtains the approval of senior management before the establishment or continuation of the business relationships with such customers;
c) Undertakes appropriate measures to identify the source of the wealth and the source of funds involved in the business relationship or in the transaction with such customers;
d) Carries out continuous and enhanced monitoring of the business relationship.

56. When identifying the customers and beneficial owners in case of transactions involving politically exposed persons, the reporting entity may request a written statement or filling in a questionnaire on the part of the customer (including prospective customer) or the representative thereof, where he/she will be invited to provide, on his/her own responsibility, sufficient information about him/her, his/her family members, related persons, the beneficial owner, the place/places of work and the position/functions held during the last 12 months, etc.

Also, in order to ensure proper/full implementation of the measures with respect to politically exposed persons, the reporting entities will apply the provisions of the Guide on identification and monitoring of politically exposed persons approved by Order of the OPFML Director No. 17 of 08 June 2018.

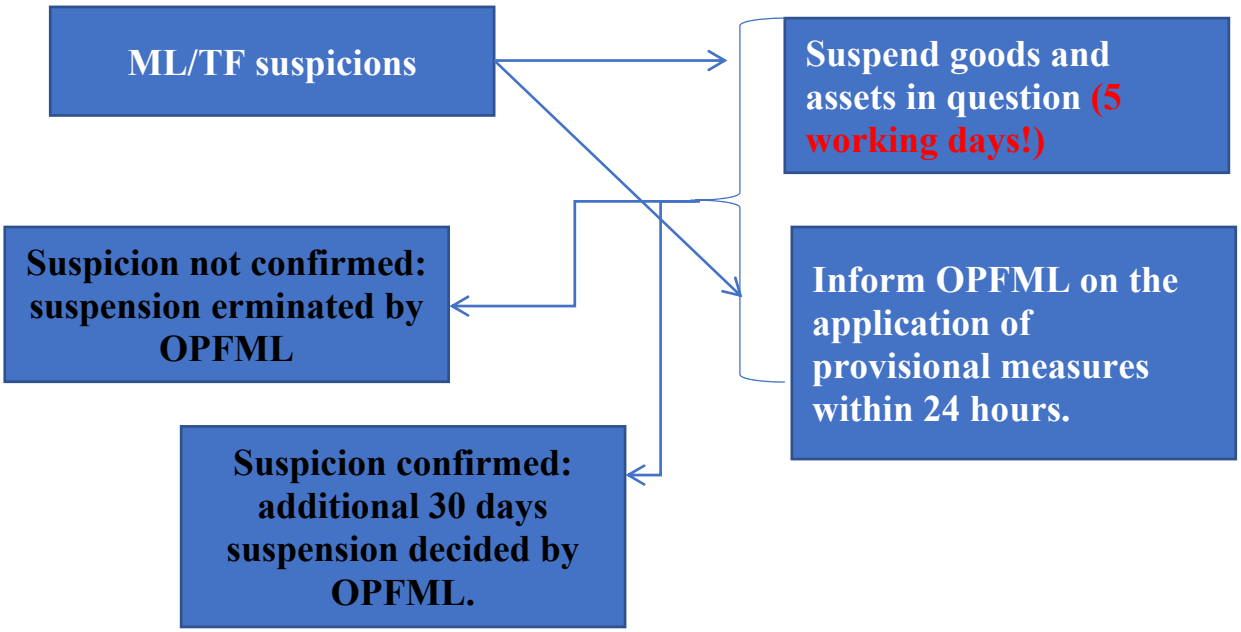
CHAPTER VII. SUSPENSION OF TRANSACTIONS

57. If the reporting entity identifies a transaction, a money laundering or terrorist financing activity or establishes substantiated suspicions as to its performance, the reporting entity is entitled to apply due diligence measures in accordance with the provisions of Art. 33 of Law 308/2017.

58. The procedure for suspension of activities and transactions is aimed at counteracting money laundering, terrorist financing or proliferation of weapons of mass destruction. This instrument involves the reporting entities, the Office, the law enforcement bodies and the judicial authorities with the primary purpose of identifying, prosecuting, stopping, where applicable, seizing by the competent authorities and eventually confiscating money/assets originating from money laundering or other offenses associated with it, terrorist financing and proliferation of weapons of mass destruction.

59. If a reporting entity identifies clear suspicions of money laundering and terrorist financing, it shall apply *ex officio* or at the request of the OPFML measures to suspend goods and assets **for up to 5 working days**, while immediately informing the Office on the application of interim provisional measures, but **not later than 24 hours**. The suspension procedure may only be terminated *ex officio* on the basis of a permission issued by the OPFML.

60. If the analysis of the received information confirms the initial suspicions, the period of suspension may be extended for **30 days** subject to a decision issued by the OPFML. The OPFML may withdraw the decision to suspend transactions with suspicious goods or assets issued before the indicated time expires if the causes and conditions which justified the issuance of such decision have ceased.



61. If needed, the Office may reasonably request the court to extend the period of application of the suspension procedure. Thus, the court, through a ruling, orders extension or rejection of the suspension. The term set out by the examining judge may not exceed **60 working days** per case.

62. The suspension decisions issued by the Office may be appealed in administrative proceedings and the ruling of the judge on the extension or rejection of the extension of the suspension term may be appealed as established by the laws, by the person who considers his/her rights have been harmed.

63. Article 33 para. (17) of Law 308/2017 also provides for certain exceptions on the application of measures to suspend activities and transactions. Under the written permission of the Office, the reporting entity may carry out the suspicious activity or transaction when it is impossible to abstain from such transactions or may create impediments to tracking the beneficiaries of a suspicious money-laundering transaction, committing of offenses, financing terrorism, or proliferation of weapons of mass destruction. These situations, however, are without prejudice to the obligations resulting from the execution of the international restrictive measures in accordance with Art. 34 of Law 308/2017.

CHAPTER VIII. REPORTING OF ACTIVITIES OR TRANSACTIONS SUBJECT TO LAW 308/2017

64. The legal provisions constituting the basis for the creation of the reporting mechanism of suspicious activities and transactions covered by Law 308/2017 are the provisions of Article 11. The reporting entities are obliged to transmit to the Office information on three types of transactions that have been classified as follows:

a) **Suspicious transactions**: to be reported by the reporting entity when identifying the criteria of suspicion with respect to goods, activities or transactions relating to attempts of money laundering or terrorist financing under preparation, planned, being completed or already completed. Suspicious transactions are reported to the Office through a special form **within at most 24 hours** from the time of identifying the circumstances giving rise to suspicion. The suspicions are established on the basis of objective and subjective criteria established in accordance with the Methodology on identification of money laundering and terrorist financing suspicious activities and transactions, approved by Government Decision No. 496 of 25 May 2018, Guide on identification terrorist financing suspicious activities and transactions, approved by Order of the OPFML Director No. 16 of 08 June 2018, Guide on identification of money laundering suspicious activities and transactions, approved by Order of the OPFML Director No. 15 of 08 June 2018.

b) **Cash transactions**: The reporting entities shall inform the Office about the activities or transactions of customers made in cash, through a transaction worth at least 100,000 MDL, or through several cash transactions that seem to have a connection between them. For this purpose, the special form shall be used and transmitted to the Office **within 10 calendar days** from the first day of the month ending on the last day of the calendar month.

c) **Transactions via transfer**: The customers' transactions through transfer worth at least 500,000 MDL shall be reported to the Office. Data on transactions via transfer shall be indicated in a special form, which shall be submitted to the Office **by the 15th of the month** following the reporting month.

65. Lawyers, notaries, accountants, auditors and real estate agents become subject to the reporting regime only during the period of participation, on behalf of the customer, in any financial and real estate transaction, or during the provision of assistance for planning or executing of transactions for the customer, in cases of sale and purchase of real estate, donation of goods, management of financial means, securities and other goods of the customer, opening and managing bank accounts, creating and managing entities, managing fiduciary goods, and their purchase and sale. Organizers of gambling and natural and dealers in precious metals and stones shall become subject to the reporting regime whenever they identify requirements that establish the reporting obligation in accordance with point 66.

66. The reporting entity reports suspicious transactions using special forms approved by Order of the Director of the Office for Prevention and Fight against Money Laundering No. 18 of 08 June 2018 on the reporting of activities or transactions covered by the Law No 308/2017. The Law also sets up the form, the structure, as well as the manner of transmission, receipt and confirmation of the special forms.

67. The special form with the necessary information is transmitted via the secure channel (secure email created for reporting purposes) to the OPFML address. In urgent cases, the information may be submitted verbally by providing data in a special form to the responsible officers of the Office in a telephone conversation after which the special electronic form is submitted via the secure channel within 24 hours after the verbal notification.

CHAPTER IX. DATA STORAGE REQUIREMENTS

68. In order to ensure smooth functioning of the regime for preventing and combating money laundering and terrorist financing, the reporting entities are required to keep all data relating to national and international transactions and activities for a period of **5 years** after the termination of the business relationship. This way, they will be able to rapidly respond to the requests of the Office and the bodies supervising the reporting entities. The stored data shall be sufficient to rebuild each transaction or activity as evidence, should this be needed in criminal, administrative and other legal procedures.

69. The reporting entities will keep all documents and information about customers and beneficial owners obtained with the application of the CDD measures, including copies of identification documents, archives of primary documents, business correspondence, results of analyses and studies conducted for identification of complex and unusual transactions for a period of 5 years for the active period of business relationship and after its termination or immediately after the date of the occasional transactions. The reporting entities shall keep records of all documents and information about transactions within 5 years after their completion, and at the request of the Office or of the supervisory entities for certain types of documents and information, the record keeping period may be extended, but for no more than 5 years.

70. The reporting entities shall have effective systems, including procedures to respond rapidly and fully to all requests and demands of the Office and the supervisory entities with respect to transactions and business relationships with customers. Also, at the request of the Office and of the supervisory entities, the reporting entities are required to provide all relevant information on business relationships with customers and on the nature of such relationships.

CHAPTER X. INTERNAL CONTROL PROCEDURES

71. An important element in ensuring implementation of the AML/CFT regime is internal control procedures. The internal control procedures are intended to ensure an appropriate level of application of legal requirements by the reporting entities in order to effectively mitigate and manage money laundering and terrorist financing risks identified at national level as well as directly by the reporting entities. Internal control policies and procedures shall therefore be commensurate to the identified risks, as well as appropriate to the specificities of the activities and the size of the reporting entities.

72. The reporting entities approve their own programs for prevention and combating of money laundering and terrorist financing, also by taking into consideration recommendations and regulatory acts approved by the supervisory bodies. The internal control procedures shall include the measures provided for in Art. 13, para. (3) of Law 308/2017, including:

a. Policies, methods, practices and written procedures for preventing money laundering and terrorist financing linked to CDD and identification and reporting and suspicious transactions and activities;
b. Updated list of names of senior staff responsible for the compliance with policies and procedures;
c. Development of ethical and professional norms in a specific sector;
d. Continuous training programmes for employees tasked with compliance duties;
e. Independent auditing and testing of compliance measures adopted in the reporting entity.

73. The reporting entities appoint persons entrusted with duties of implementing the AML/CFT related legislation, including those holding senior management functions whose name shall be communicated within **5 working days** to the Office and the supervisory bodies, together with the nature and limits of responsibilities. The indicated persons as well as other responsible employees shall have access to the results of the CDD measures, including to the identification data and details on transactions and activities carried out, as well as other necessary relevant information.

74. The reporting entity shall take appropriate steps to remedy vulnerabilities if the results of verifications carried out by the supervisory bodies have established such circumstances. This also applies when suspicions on the reliability of responsible persons arise. If the person responsible for ensuring compliance of policies and procedures with AML/CFT requirements has not been appointed, such responsibilities are directly taken over by the head, and in the absence thereof, by his/her alternative.

CHAPTER XI. APPLICATION OF INTERNATIONAL RESTRICTIVE MEASURES

75. A number of treaties signed by the Republic of Moldova and certain decisions of international organizations have elements of implementation of restrictive measures or financial sanctions against particular persons, groups or entities. In order to create a clear vision of how the Republic of Moldova has to implement the international treaties or the decisions that have the nature of application of restrictive measures, the Law No. 25 of 04 March 2016 ‚On the application of international restrictive measures' was adopted. This normative act governs the way of introducing, applying and removing the restrictive measures established by the resolutions of the United Nations Security Council, through the acts of the European Union to which the Republic of Moldova has aligned through the acts and decisions adopted by other international organizations or by other states to which the Republic of Moldova has aligned itself, and last but not least, by the Republic of Moldova on its own initiative.

76. Implementation of these restrictive measures is also part of the regime for prevention and combating of money laundering and terrorist financing. In this respect, the international financial sanctions are binding and are directly applicable throughout the Republic of Moldova. The sanctions above are intended to eradicate and counteract worldwide actions aimed at facilitating terrorist activities and proliferation of weapons of mass destruction. To ensure effectiveness of these restrictive measures, they are specifically directed against individuals, groups and entities that may be involved in such actions.

77. Persons, groups and entities involved in terrorist activities or activities of proliferation of weapons of mass destruction are included in special lists published in order to facilitate the implementation of sanctions by states that are signatories to international treaties. In the case of the Republic of Moldova, there are four basic lists to be taken into consideration by the reporting entities. The Intelligence and Security Service is the authority that publishes on a regular basis the consolidated list (consisting of the 4 lists) of individuals, groups and entities involved in terrorist activities and proliferation of weapons of mass destruction.

78. The reporting entities are required to immediately apply restrictive measures with respect to goods, including those obtained from or generated by goods owned or held or controlled, directly or indirectly, by the persons, groups and entities included in the consolidated list, as well as by legal entities that are owned or controlled, directly or indirectly, by such persons, groups and entities. The reporting entities also refrain from activities and transactions in favour or for the benefit, directly or indirectly, of the persons, groups and entities included in the consolidated list, as well as of the legal entities that are owned or controlled, directly or indirectly, by these entities persons, groups and entities.

CHAPTER XII. SANCTIONS

79. Violation of the provisions of the AML/CFT related legislation shall, as the case may be, entail disciplinary, pecuniary, administrative, criminal or other liability in accordance with the laws in force.

80. The sanction mechanism is provided in Art. 35 of Law 308/2017 stipulating the criteria, actions and procedure for imposing sanctions on the reporting entities.

81. When imposing sanctions, severity, duration and frequency of the violation, intention, degree of responsibility, financial capacity of the subject, benefit obtained from the violation, damage to third parties through violation, cooperation of the subject, previous violations shall be taken into account.

82. In case of failure to comply with the requirements, the reporting entities are subject to the following types of sanctions:

a) A public statement in the media identifying the natural or legal person and the nature of the violation;
b) A prescription requiring the natural or legal person to cease the behaviour concerned and to refrain from repeating it;
c) Withdrawal or suspension of the authorization, license of activity, if the activity of the reporting entity is subject to authorization or licensing;
d) Temporary prohibition on exercising senior management positions in the reporting entities by any person with senior management functions in a reporting entity or by any other natural person held liable for the violation;
e) Financial sanctions in the form of a fine double the value of the benefit resulting from the violation of the AML/CFT obligations, if the respective benefit can be established, or in the amount of the MDL equivalent of the sum up to 1,000,000 EUR, calculated according to the official exchange rate of Moldovan currency at the time of the violation.

83. The application of the sanctions will be subject to the Law on the procedure for detection of violations of money laundering and terrorist financing and the manner of application of the fine, which will constitute the main legislative basis governing the application of penalties in the field of prevention and combating of money laundering.

84. At the moment, the administrative liability is regulated by the Contraventional Code at art. 291^2-291^9 where are stipulated the violations and sanctions currently applicable in the field of money laundering and terrorist financing are stipulated.

85. After the adoption of the Law on the procedure for detection of violations of money laundering and terrorist financing and the manner of application of the fine the provisions of the Contraventional Code will be cancelled.

Appendix No. 1.

AML/CFT Test: how much do you know?

1. What supervisory entities control the enforcement of the laws on prevention and combating of money laundering by lawyers and notaries?

- Enforcement of the laws on prevention and combating of money laundering and terrorist financing by lawyers is supervised by the **Lawyers Union of the Republic of Moldova** and by the **Notary Chamber** in the case of notaries.

2. What are the actions to be taken by the supervisory bodies if, following some inspections or otherwise they detect actions that may be related to money laundering or terrorist financing?

- If following inspections or otherwise, the supervisory authorities detect actions, activities or facts likely to be related to money laundering or terrorist financing, they shall immediately, but **not later than 24 hours**, inform the Office while submitting to this end the necessary information and documents.

3. What is the purpose of applying the risk-based approach?

- The purpose of the risk-based approach is used to develop actions for prevention and mitigation of money laundering and terrorist financing that are commensurate to the risks identified. This approach also allows for efficient allocation of available resources.

4. Who is responsible for assessing money laundering and terrorist financing risk at the national level?

- The Office, jointly with the bodies supervising the reporting entities, the law enforcement bodies and other competent institutions.

5. In what situations enhanced CDD measures shall be applied?

- The reporting entities apply enhanced CDD measures in situations where, by their nature, customers may present an increased money laundering or terrorist financing risk (for instance with PEPs), as well as in other situations, subject to criteria and factors set by the supervisory bodies.

6. What is the time period for which the reporting entities may suspend activities or transactions that meet clear criteria of suspicion of money laundering or terrorist financing?

- The reporting entities may *ex officio* or on request suspend activities and transactions with goods, including financial means, for **up to 5 business days**, if they find relevant AML/CFT related suspicions.

7. What is the time period established for the reporting entities to send special forms on cash transactions?

- Data on cash activities or transactions are sent to the Office within **10 calendar days** starting from the first day of the reporting month and ending with the last day of the calendar month

8. What kind of documents shall be kept by the reporting entities in order to comply with the data storage requirements and what is the time period for which this information shall be kept?

- The reporting entities will keep all documents and information on customers and beneficial owners obtained through CDD measures, including copies of identification documents, archives of accounts and primary documents, business correspondence, results of analyses and studies conducted on the identification of complex and unusual transactions during the active period of the business relationship and for a period of **5 years** after its termination or after the date of occasional transactions.

9. What forms of sanction can be applied by the Office for Prevention and Fight against Money Laundering and the supervisory authorities to the reporting entities for their failure to comply with the AML/CFT requirements?

The Office and the supervisory authorities may apply the following forms of sanction:

a) A public statement in the media identifying the natural or legal person and the nature of the violation;

b) A prescription requiring the natural or legal person to cease the behaviour concerned and to refrain from repeating it;

c) Withdrawal or suspension of the authorization, license of activity, if the activity of the reporting entity is subject to authorization or licensing;

d) Temporary prohibition on exercising senior management positions in the reporting entities by any person with senior management functions in a reporting entity or by any other natural person held liable for the violation;

e) Financial sanctions in the form of a fine.

10. What are the persons, groups and entities to which the reporting entities shall apply restrictive measures?

- The reporting entities will apply **international restrictive measures** to those who are included in the following lists:

  a) The United Nations Security Council list on persons, groups and entities involved in terrorist activities;

  b) The United Nations Security Council list on persons, groups and entities involved in activities of proliferation of weapons of mass destruction;

  c) The European Union list on persons, groups and entities involved in terrorist activities;

  d) Supplementary list of the Information and Security Service on persons, groups and entities involved in terrorist activities.

  The reporting entities are encouraged to follow the official websites of the United Nations, the European Union and the Intelligence and Security Service for updated information.

11. Once the reporting entities have appointed the persons authorized to implement AML/CFT provisions, what actions shall be undertaken?

- After the appointment of the authorized persons, the reporting entity shall communicate their names, the nature and the limits of their responsibilities within **5 working days** to the Office and to the supervisory bodies.

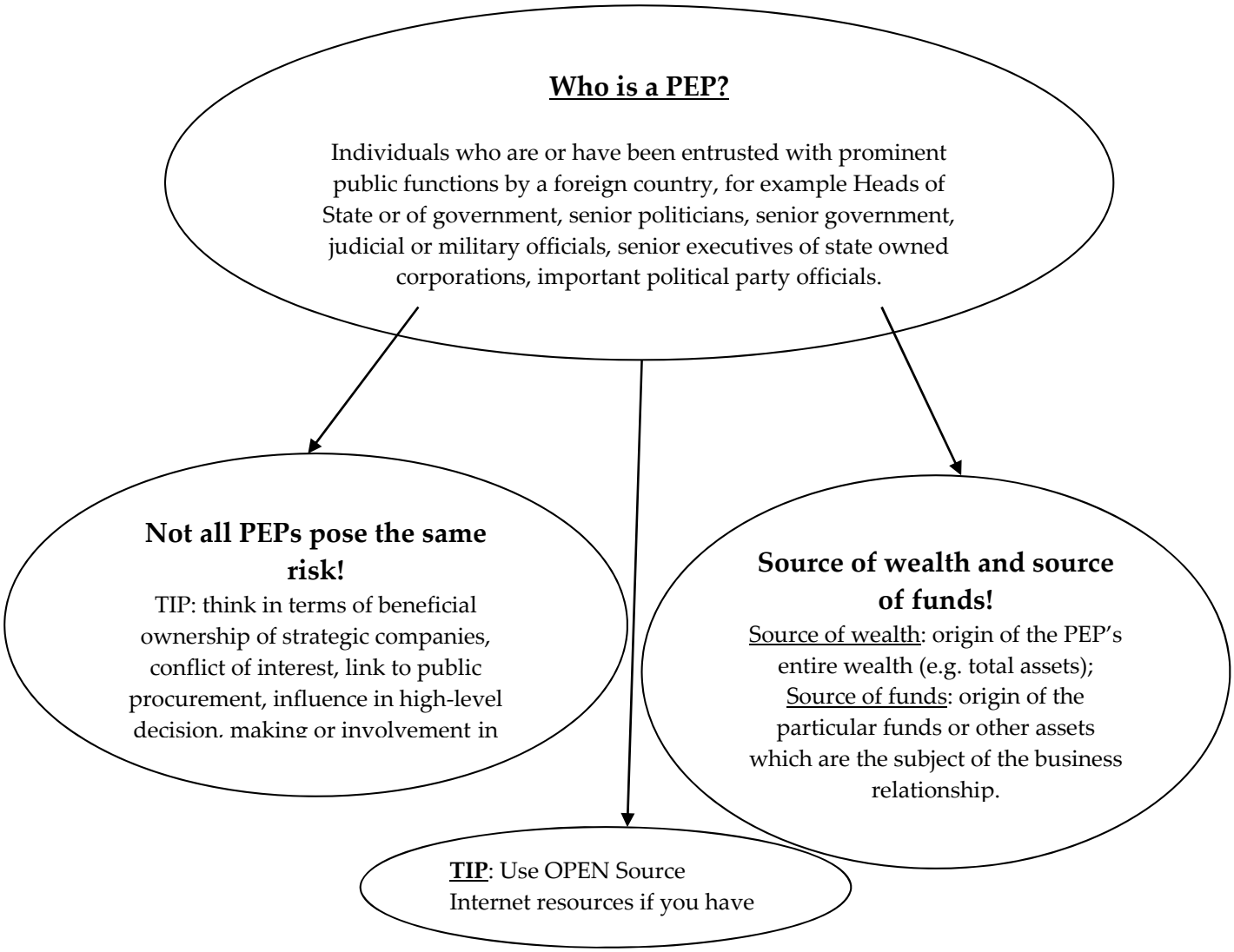
Appendix No.2
Summary: what do you need to do to comply?

The table below describes the ideal steps to be taken to comply with AML/CFT requirements. It represents a summary of AML/CFT requirements. More details can be found in the AML/CFT Law No. 308/2017 and in the guidelines issued by the Office.

Step 1: Establish a compliance programme
Appoint a compliance Office, if the size of your company allows for it. If this is not possible, the sole person responsible for the company will need to deal with compliance matters.
Conduct a risk assessment: you are required to conduct an assessment of the money laundering and terrorist financing risk involving your business. The NAR can give good indications. The assessment should be in writing and forwarded to the supervisory entity.
Develop an AML/CFT Programme: based on the risk assessment performed, a series of actions shall be designed to counteract the vulnerabilities. They can be elucidated in policies and procedures to disseminate in the company to increase compliance.
Step 2: Maintain the compliance standards
As explained above, different due diligence shall be applied to clients with different features. CDD should be an on-going process that applies also to existing customers, in an effort to regular review the risks posed. CDD can be simplified, standard or enhanced.
Keeping records of suspicious transactions and activities as well as the verifying documents for each customer is an essential step. Documents must be kept for at least 5 years and made readily available.
Initial CDD is not sufficient to ensure compliance. It needs to be a continuous process of monitoring and update, when necessary. This will facilitate the identification of suspicious activities.
The risk assessment and the measures set to respond to its results need to be reviewed and adjusted to possible emerging AML/CFT risks and trends.
Step 3: Report and audit
Suspicious transactions and activities reports must be timely submitted to the Office, according to the deadlines set in the Law No. 308/2017.
Risk assessment and internal control procedures shall undergo an annual independent auditing and testing of the compliance measures adopted in the reporting entity.

Appendix No. 3.

Politically Exposed Persons, tips for effective implementation:



Who is a Beneficial Owner?

FATF: Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

!

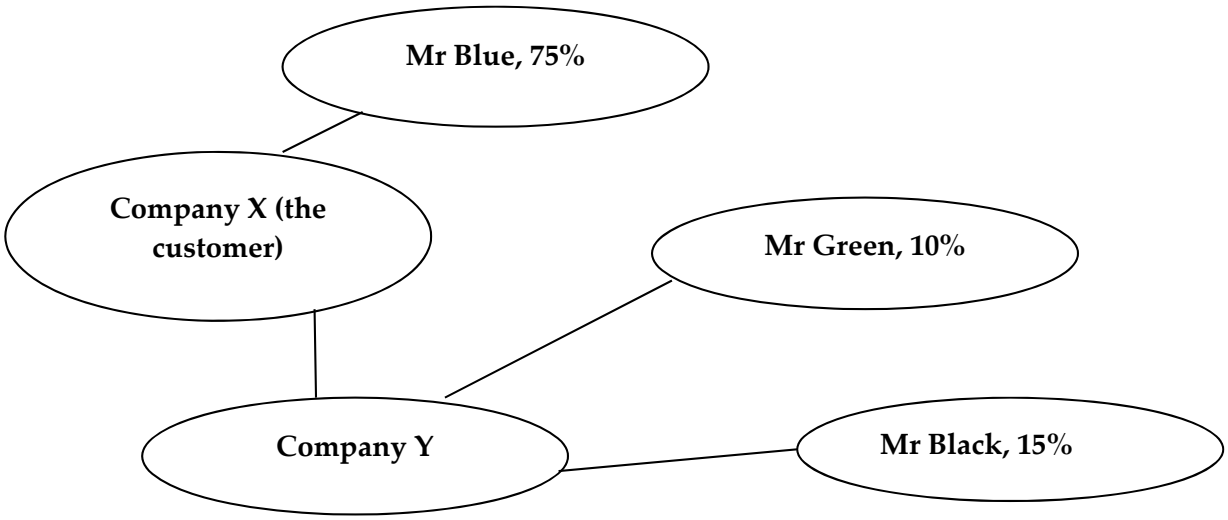
Key questions:

4) Who owns more than 25% of the company/business?
5) Who has effective control over it?
6) Who is the person on whose behalf transactions are conducted?

How to identify the ultimate beneficial owner?

- ✓ Build a robust framework to ensure compliance;
- ✓ Consult official national registries, when available;
- ✓ Look for information on the beneficial owner, but also on the intermediaries;
- ✓ Use online sources of information;
- ✓ Determine and understand the organizational structure of the client;

An example: Company X is owned by Mr Blue, who owns 75%, and is equally owned by two other individual, Mr Green and Mr Black. Assuming this ownership structure is correct, the identity of the individuals owning more than 25% shall be clarified.



Appendix No. 4.

Types of money laundering and terrorist financing associated with the reporting entities

a. **Lawyers and notaries**

As FATF studies have observed, while not all legal professionals are actively involved in providing these legitimate legal services which may be abused by criminals, the use of legal professionals to provide a veneer of respectability to the client's activity, and access to the legal professional's client account, is attractive to criminals. There is also a perception among criminals that legal professional privilege/professional secrecy will delay, obstruct or prevent investigation or prosecution by authorities if they utilise the services of a legal professional. Criminals may also seek out the involvement of legal professionals in their ML/TF activities, sometimes because a legal professional is required to complete certain transactions, and sometimes to access specialised legal skills and services assisting in the laundering of the proceeds of crime. The ML risk is more relevant when the lawyer is offering these types of services:

- Creating and managing resident and non-resident legal entities with complex ownership structure;
- Facilitating or carrying out financial transactions on behalf of other persons;
- Receiving and transferring large amounts of cash;
- Forgery of documents;
- Establishing loan agreements or complex financial arrangements;
- Facilitating the transfer of ownership rights to intermediaries or persons with false identity documents.

An example of a real case identified in Belgium[10] is presented below. The case involves the use of a legal professional to undertake financial transactions, unrelated to the provision of legal services, to hide funds from a bankruptcy:

A trading company, operated by the client's spouse, was declared bankrupt. Shortly afterwards the client deposited cash (from the bankrupt company) in an account opened in the name of a family member. The money was immediately paid by cheque to the account of a legal professional. The legal professional deposited part of the funds back into the family member's account and used the rest to purchase a life assurance policy, via a bank transfer. The policy was immediately cashed in by the family member.

What are the Red Flag indicators?

• Private expenditure is being funded by a company;

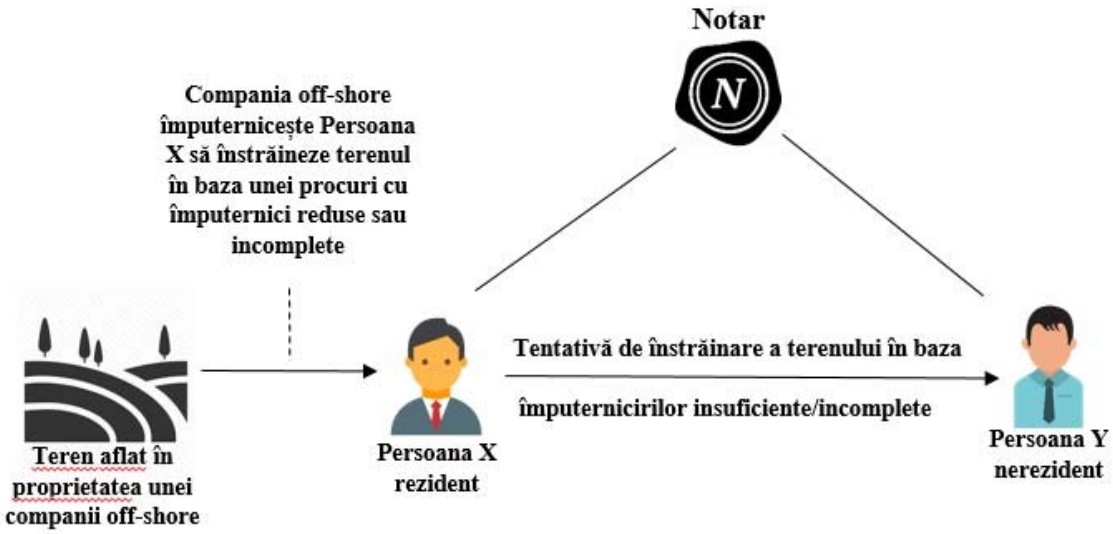
• The transaction is unusual in terms of funding arrangements, who the client is, and the reason for the involvement of the legal professional;

• The use of "U-turn" transactions where money is transferred to a legal professional or other entity and then sent back to the originating account in a short timeframe;

• Insurance policies cashed in shortly after purchase or loans and mortgages paid quickly, in full;

As representatives of liberal professions, notaries can identify throughout their activity a series of clearly suspicious transactions; an example of such a transaction is presented below.

[10] Source: FATF and Belgium.



An offshore company owning a land plot in the Republic of Moldova authorizes Person X who is a resident of the Republic of Moldova to sell the plot on behalf of the company. Person X appears at a notary together with Person Y who wants to acquire the plot. Following the verification of the required documents, the notary observes that the power of attorney issued by the offshore company does not include sufficient or complete data to enable Person X to alienate the property, or the power of attorney is not authenticated and certified in the manner established by the law. The notary also notes that the person who appears as a buyer is a foreign national.

What are the Red Flag indicators?

• Use of an offshore company;

• Incomplete information, which may raise the suspicion about the use of a front man.

Another real case from France[11] relevant to the Republic of Moldova is explained below:

A foreign client approached a legal professional to buy two properties, one in Alpes-Maritimes (South of France), and another one in Paris, for a total of 11 million EUR. The purchase price was completely funded by the purchaser (there was no mortgage) and the funds were sent through a bank in an off-shore jurisdiction. As the contract was about to be signed, there was a change in instructions, and a property investment company was replaced as the purchaser. The two minor children of the client were the shareholders of the company. The foreign client held an important political function in his country and there was publicly available information about his involvement in financial wrongdoing.

What are the Red Flag indicators?

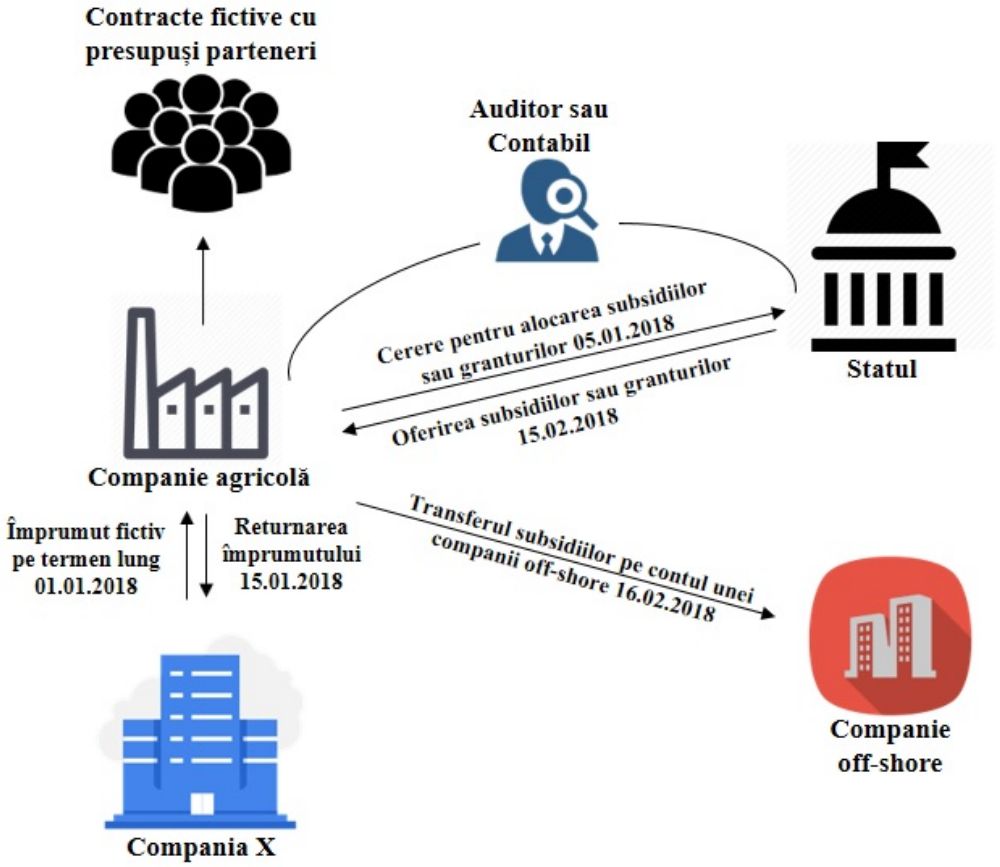
• Disproportionate amount of private funding which is inconsistent with the socio-economic profile of the individual;

• Client is using bank accounts from a high-risk country;

b. Accountants and Auditors

[11] Source: FATF and France.

There are many examples in which auditors or accountants can be used directly or indirectly to commit financial frauds and launder money, given that most of the companies' financial transactions are accessible to representatives of these professions. An example where both accountants and auditors can be involved is provided below.



In order to obtain non-reimbursable subsidies or grants from the state, an agricultural company obtains a long-term loan from Company X. The purpose of the contract is to mitigate the significant presence of funds on the accounts of the agricultural company. Consequently, this amount of money is returned to Company X, after a short period of time. The next step is signing fake contracts with hypothetical customers to create the impression that the agricultural company has many distribution channels for agricultural products. Then the agricultural company submits the set of documents required to receive subsidies or grants from the state. This set of documents may contain other fake, semi-fake or even authentic documents to convince the state or other institution to provide the necessary amount of money. Once the funds are received in the form of non-reimbursable subsidies or assistance, the agricultural company transfers this amount to the account of the offshore company under a fake contract for purchase of agricultural equipment or machinery. It is worth mentioning that in some cases, in order to receive financial assistance in the form of subsidies or grants, an audit report is required. Therefore, the auditors and accountants are those who have access to certain types of documents and by virtue of their functions can decipher suspicious activities of financial fraud.

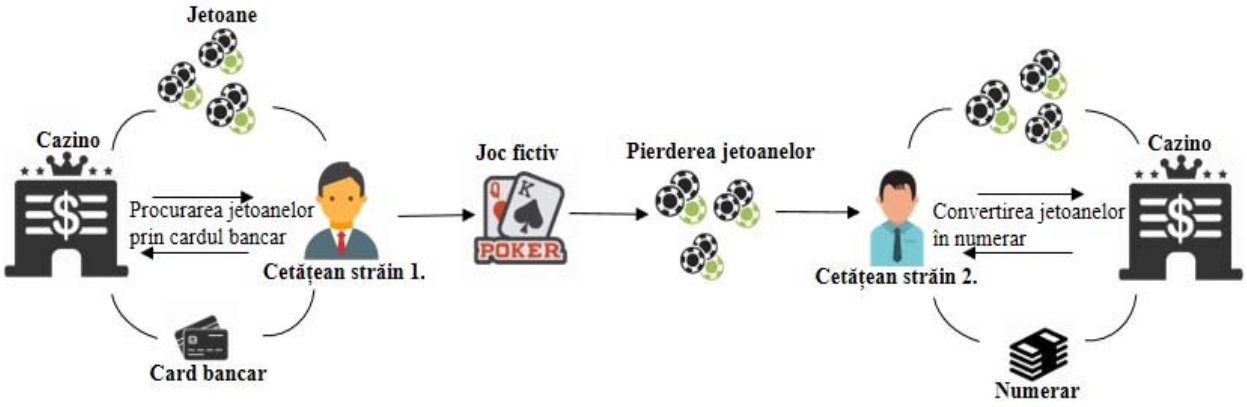
What are the Red Flag indicators?

- Anomalous transactions;
- Use of offshore companies;
- Use of forged or fake documents.

c. Casinos and other gambling service providers

Casinos and other gambling service providers can be used to launder money, especially when cash needs to be legalized under the cover of winnings in gambling, or through the purchase of chips without engaging in gambling activities (or just conducting minimal activities). In several jurisdictions it has also been observed that usury ("loan sharking") is also a risk in many casinos.

A possible money laundering scheme is shown in the picture below.



Foreign national 1 purchases from a Casino with a bank card chips below the mandatory limit of reporting to the Office. These chips can be also purchased over several days. Consequently, the Foreign national 1 sits at the table, assuming an appropriate behaviour to disguise his intentions. Over a certain period of time Foreign national 1 loses the accumulated chips to Foreign national 2 following a special scheme established in advance. Thus, Foreign national 2 gaining chips converts them into cash. To avoid suspicion, Foreign national 2 will convert the chips gradually so as not to exceed the required reporting limit.

What are the Red Flag indicators?

- Use of „smurfing" (breaking down transactions below the reporting threshold to avoid detection and reporting;

Another real case from Spain[12], involving the purchase of chips and gambling with minimal gambling, is presented below:

Different people entered separately in a casino and bought chips. After playing minor amounts of chips they tried to change chips and requested a cheque paid to the name of a third person. They tried to do the same operation with different people and lower amounts one day later, which raised suspicion of casino operators.

What are the Red Flag indicators?

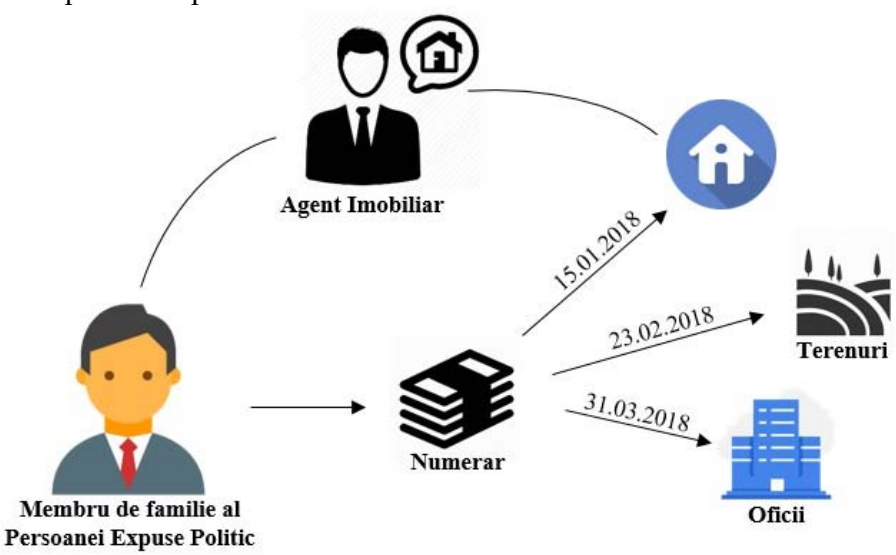
- Purchase of chips without gambling;
- Use of third parties (different from the person who purchased the chips);
- Reimbursement of the chips with different mean than the one used for purchase;
- Possible „smurfing".

d. Real Estate Agents

The real estate sector is an attractive target for people trying to conceal illegally obtained financial means. Real estate offers the possibility to legalize very large amounts of cash through just one

[12] Source: FATF and Spain;

transaction. According to the FATF, buildings are the third in terms of the value of illicit assets seized worldwide. The new AML/CFT provisions oblige the legal and physical persons acting as realtors to apply due diligence to their customers in a more detailed manner. Thus, the reporting entities working in the real estate sector need to be prepared for the legislative changes. A concrete example where a real estate agent can identify criteria of suspicion with respect to his/her customer who buys a range of real estate properties both for residential and commercial purposes using cash for that purpose is provided below. Such situations can occur after establishing business relationships with a particular customer.



Immediately after setting up business relationships, following the application of due diligence measures to one of the customers, the real estate agent who assists in purchasing a property discovered that his/her customer is a family member of a Politically Exposed Person. The real estate agent noticed that his/her customer had acquired in a short period of time several real estate properties, including commercial buildings, farmland, construction sites and a residential property. The customer made payments in cash, which raise high suspicions considering that such properties are expensive. In this context, such transactions involve several criteria of suspicion to be taken into account by real estate agents.

What are the Red Flag indicators?

- Transactions may not be consistent with client's economic profile, suggesting the use of a „front" (the family member, to hide the link to the PEP);
- Use of cash;

Another example where the real estate agent identified a series of suspicious transactions is similar to that one above, but in fact took place outside the Republic of Moldova:

A 19-year-old person living in a provincial area turned to a real estate agent to acquire a range of properties in the central area of a large city. The real estate agent found it suspicious that a person with such a profile is willing to acquire high-value commercial properties. Thus, along with provision of assistance services in identifying potential properties, the real estate agent has notified the authority responsible for preventing and combating money laundering in that country. Following the necessary investigations, the authorities found that the 19-year-old person was the daughter of a drug dealer who legalized the profits obtained illegally through his daughter.

Red flag indicators:

- Transactions may not be consistent with client's economic profile, suggesting the use of a „front".

e. Luxury Goods Dealers

The main market for luxury goods are developed countries. However, emerging markets and new economies are also affected by the expansion of this sector, which provides above-average profits. An example of a case is presented below:

Mr X was a high-level politician in Country Y. Mr X and his staff accumulated money and assets abroad in the course of their political mandate. Mr X and his relatives also owned 220 companies which covered about 25% of Country Y's private sector. Luxury assets including sport cars, yachts, fine art, jewellery and palaces (over 12,000 items!) belonging to Mr X were all of a sudden auctioned. Officials declared that the assets valued in total over (€400 million) and were bought systematically to launder the money obtained through corruption during Mr X's political career[13].

What are the Red Flag indicators?

• Luxury items inconsistent with economic profile of the client;

The case below illustrates a scheme involving a diamond trading company, with links to terrorist financing.

The Financial Intelligence Unit (FIU) in Country M received suspicious transactions reports from different banks. The reports concerned two natural persons and a diamond trading company. All three were account holders in the banks and in the course of few months, large amounts were transferred to and from foreign accounts. One of the accounts held by the company received large deposits in foreign currency originating from other companies active in the diamond industry. The transfers were consequently converted in local currency and transferred again to foreign accounts, especially to an account in Country G registered to one of the individuals mentioned above. FIU discovered that an investigation for diamonds trafficking had been already opened by the police in Country M. The company and the individuals involved were suspected of buying diamonds from different companies (probably linked to armed conflict areas), resell them and disguise the movements of cash with transfers between domestic and foreign accounts and changes of currency. Further research by the FIU also revealed links between the subjects of the suspicious transaction report and the individuals and companies already tied to the laundering of funds for organised crime and terrorist financing[14].

What are the Red Flag indicators?

• Use of several companies, located in different jurisdictions to disguise beneficial ownership and links to funds;

[13] Egmont Group, Tunisia.

[14] FATF;