GOOD PRACTICES IN ANTI-MONEY LAUNDERING

BULGARIA, MALTA AND THE NETHERLANDS

Erasmus+ Project № 2019-1-BG01-KA204-062575
Cooperation for innovation and exchange of good practices in the fight against Money Laundering
(The Republic of Bulgaria)

I. INTRODUCTION

1. Introducing phrase

Hereby we present you a list with definitions, concerning the area of money laundering and financing terrorism. These definitions may serve you as a guideline, while exploring our next topics.

Money laundering Vocabulary

1. **Money laundering** – means illegal process of making large amounts of money generated by a criminal activity, such as drug trafficking or terrorist funding, appear to have come from a legitimate source. The money from the criminal activity is considered dirty, and the process "launders" it to make it look clean.

2. **Terrorism** – means any act of a criminal nature accompanied by an act of violence, which by endangering the safety and lives of citizens, as well as important infrastructure sites, aims to create fear and insecurity in society and to destabilize institutions as a means to achieve specific political and ideological goals.

3. **Terrorism financing** – means the raising, moving, storing and using of financial resources for the purposes of terrorism.

4. **Know your customer** – means the process of identification and verification of the identity of a client in which a series of controls are applied to avoid having commercial relations with people related to terrorism, corruption or money laundering, among others.

5. **High risk countries** – means countries or jurisdictions with serious strategic deficiencies to counter money laundering, terrorist financing, and financing of proliferation.

6. **High risk third countries** - third-country jurisdictions which have strategic deficiencies in their national AML/CFT regimes that pose significant threats to the financial system of the Union.

7. **Obligated persons** – means persons who must comply with the measures against money laundering.

8. **Competent authority –** means a national authority, responsible to ensure the proper conduct and compliance with the AML measures by the obliged persons. The competent authorities are entitled to make revisions and impose the sanctions for non-compliance, determined by the AML legislation.

9. **Beneficial ownership** – means a term in domestic and international commercial law which refers to the natural person(s) 'who ultimately own or control a legal entity or arrangement, such as a company, a trust, or a foundation'.

10. **Beneficial owner -** means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted.

11. **Property** - means assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets.

12. **Criminal activity –** means any type of criminal activity related to crimes such as: crimes related to terrorist activities, fraud affecting the Union's financial interests, corruption, tax crimes relating to direct taxes and indirect taxes and etc.

13. **Credit institution –** means an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account.

14. **Financial institution –** means an undertaking other than a credit institution which carries out activities such as: lending, financial leasing, payment services, portfolio management and consulting, storage and management of securities, issuance of electronic money ant etc.

15. **Shell bank**- means a credit institution or financial institution, or an institution that carries out activities equivalent to those carried out by credit institutions and financial institutions, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

16. **Parent undertaking** – means a legal entity a legal entity that exercises control over one or more subsidiaries (subsidiary companies).

17. **Subsidiary** – means a legal entity which is controlled by another legal entity, known as parent undertaking.

18. **National risk assessment –** means a holistic risk assessment which analyses the internal and external risks of money laundering and financing terrorism. Every Member State is obliged to adopt a national risk assessment. The National Risk Assessment aims to take measures against money laundering and financing terrorism on a national level. The National Risk Assessment is based on the Supranational Risk Assessment. The Obliged parties shall use the National Risk Assessment of their country as a basis for their internal rules and terms, concerning AML compliance.

1. ***Definition of Money Laundering in Buglaria according to the law, according to the court jurisprudence.***

- **Definition of money laundering according to Measures Against Money Laundering Act in Bulgaria**

Money laundering in the meaning of Measures Against Money Laundering Act, where it has been committed intentionally shall be:

1. reformation or transfer of property with the awareness, that this property has been acquired from crime or from an act of participation in a crime, in order to be hidden or disguised the illegal origin of the property or on order to support a person, who participates in committing such an action in view to avoid the legal consequences from the deed of this person;

2. hiding and disguising the nature, source, location, movement, the rights in relation to or the ownership over the property with the awareness that this property has been acquired from crime or from an act of participation in a crime;

3. acquisition, possession, holding or using of property with the awareness at the moment of receiving, that it has been acquired from crime or from an act of participation in a crime;

4. participation in some of the actions under p. 1 – 3, association in view to committing such an action, the attempt to carry out such an action, as well as support, incitement, facilitation, or giving advice while committing such an action or its hiding.

Also according to Art.2, para 2 of MMLA money laundering is: The knowledge, intent or purpose required as an element of those specified in para. 1 activities may be established on the basis of objective factual circumstances.

Money laundering is also present where the activity, from which the property under Para. 1 has been acquired, has been committed in another Member State, or in a third state and does not fall under the jurisdiction of the Republic of Bulgaria.

- **Definition of money laundering according Bulgarian Criminal Code**

"Money laundering" has two main criminal groups under Art.253 para 1 and para 2 of Bulgarian Criminal Code. It is a crime against the financial system and the aim of the crime is to legalize illegally acquired income.

Under Art.253, para 1 of Bulgarian Criminal Code: "Whosoever carries out a financial operation or a transaction with a property, or hides the origin, location, movement or actual rights on a property about which he knows or suspects that they have been acquired through a crime or another socially dangerous act, shall be punished for money laundering."

Under Art.253, para 1 of Bulgarian Criminal Code: "those who acquire, receive, keep, use, transform or contribute in any way for the transformation of a property for which he knows or suspects by the moment of its receipt that it has been acquired through a crime or another socially dangerous act."

The punishment is: "***imprisonment of one to six years and a fine of three thousand to five thousand levs."***

- **Definition of money laundering according to Bulgarian court jurisprudence**

According to Bulgarian criminal law, the crime affects public relations, which impedes the entry into the financial system and the movement in its illegal assets. In this sense, understanding of its immediate object in the case law is almost clear:

"Money laundering may be defined as an act which (by its nature) is intended or has the effect of making it difficult for the authorities to ascertain the illegal origin of the property, respectively the real rights of the persons having such property in the respective sites." ***(DECISION No 131/24 July 2012, criminal case No 427/2017, Supreme Court of Cassation)***

"... the essential characteristic of money laundering defines it as an economic activity, with a view to concealing the criminal origin of the benefit of the' original crime ', or to operating it so as to be legally acquired and legalized in the economic, business and financial." ***(DECISION No 148/21 October 2016, criminal case No 558/2016, Supreme Court of Cassation)***

"... 'money laundering' is a criminal activity for the purpose of legalizing criminal assets and property intended and leading to the obstruction or at least making it difficult for the authorities to establish the illegal origin of the crime." ***(DECISION No 309/11 April 2018, criminal case No 1156/2017, Supreme Court of Cassation)***

"..."money laundering" is complicated activity, the crime being formal and deemed complete with the commission of the act without the necessity of a definite criminal result. It is sufficient to carry out some of the activities specified in the provisions of the law, for to bring criminal responsibility for the perpetrator. It should be established by only the connection between the object of the crime and the initial crime." ***(DECISION No 12/19.03.2012, criminal case No 2229/2011, Supreme Court of Cassation)***

"The subject of the crime under Art.253 of the CC, apart from money, can be any movable property, real estate and property and property rights or other rights thereto, acquired from a previous criminal or public danger activity, i. this act is a secondary crime." ***(DECISION No 148/21 October 2016, criminal case No 558/2016, Supreme Court of Cassation)***

"Money laundering is possible with active actions of the perpetrator only, which make it difficult for the authorities to identify the illegal origin of the property, respectively of the actual rights of persons over the criminalized property." ***(DECISION No 450/22 February 2011, criminal case No 2110/2011, Supreme Court of Cassation)***

It is settled in the legal theory and the court jurisprudence that money laundering is a formal crime and it is completed with the commission of the act without the need for a definite criminal result. The object of the crime is the lawful functioning of the country's financial system. From an economic point of view, the financial system of a country is a set of relatively separate cash

flows or financial relationships, and in institutional terms, a set of institutions that regulate, implement, manage and control financial relations.

There are two types of financial relations:

- fiscal financial relations, which cover the revenues and expenditures of the state (budget), and
- non-fiscal ones, expressing the revenues and expenditures of legal entities and individuals.

Both types of financial relationships can be a subject of money laundering.

2. ***Hereby we present the money laundering definitions, adopted by the Directive (EU) 2015/849 and some leading European countries***

➢ Definition in Directive (EU) 2015/849 of The European Parliament and of The Council

The Directive (EU) 2015/849 of The European Parliament and of The Council (referred to hereinafter as the '**Directive**') contain a detailed definition of money laundering.

According to Art. 1, Para 3 of the Directive:

'*For the purposes of this Directive, the following conduct, when committed intentionally, shall be regarded as money laundering:*

(a) the ***conversion or transfer of property****, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;*

(b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;

(c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;

(d) *participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c)*'.

➢ Definition of money laundering in Germany

The definition of money laundering in Germany is set out in Art. 261, para 1 of the German Criminal Code (StGB).

The definition is, as follows:

'*Whoever **hides an object derived from one of the unlawful acts** referred to in sentence 2, **conceals its origin, or obstructs or endangers the investigation of its origin, its being found, its confiscation** or its being secured incurs a penalty of imprisonment for a term of between three months and five years*.'

Exploring the aforementioned Article of the Criminal Code, we can conclude that in Germany money laundering is: **the act of hiding an object, derived from one of the unlawful acts, concealing its origin, or obstructing or endangering the investigation of its origin and the possibility for its finding, security and confiscation**.

- **Definition of money laundering in France**

The French definition of money laundering is set out in the French Criminal Code.

According to Art. 324, Para 1 of the French Criminal Code:

*'Money laundering is facilitating by any means the **false justification** of the origin of the **property or income** of the perpetrator of a felony or misdemeanour which has **brought him a direct or indirect benefit**. Money laundering also comprises assistance in investing, concealing or converting the direct or indirect products of a felony or misdemeanour.'*

- **Definition of money laundering in Italy**

The definition of money laundering is provided for in Art. 648 of the Italian Criminal Code (ICC) , which incriminate the actions of anybody who '*with **knowledge and intent**, **substitutes or transfers money, goods or other things of** value deriving from **an intentional crime** or carries out, in relation to that benefit, any transactions in such a way as to obstruct the identification of their criminal provenance*.'

Thus, we can conclude that the Italian definition of money laundering is: **informed and intentional substitution or transfer of money, goods or other things of value deriving from an intentional crime or carrying out for benefit any transactions in such a way as to obstruct the identification of the criminal provenance**.

- **Definition of money laundering in England**

The English definition of money laundering in England is given by the Financial Intelligence Unit for National Instant Criminal Background Check System, London, and it states that:

'*Money-laundering is a **processing of proceeds of crime where criminals try to disguise their illegal origin**. Once such process is successfully carried out (the proceeds are "laundered"), **criminals can use these monies legitimately without revealing their original source***.'

- **Definition of money laundering in Austria**

Money laundering in Austria is defined under Art. 165 of the Austrian Criminal Code (StGB).

The definition is, as follows:

'*Money laundering § 165.*

(1) Anyone who conceals or hides any part of his or her assets that result from an act threatened with more than a year in prison or an offense pursuant to Sections 223, 229, 289, 293, 295 or Sections 27 or 30 of the Narcotics Act, Veiled origin, in particular by providing false information in legal transactions regarding the origin or the true nature of these property components, the property or other rights to them, the power of disposal over them, their transfer or where they are located, is imprisoned punishable to three years.

(2) Anyone who knowingly acquires, stores, invests, manages, converts, exploits or transfers to a third party that knowingly comes from an act of another specified in paragraph 1 shall also be punished.

(3) Also punishable are those who knowingly bring assets of a criminal organization (Section 278a) or a terrorist organization (Section 278b) that are subject to, on their behalf or in their interest, safekeeped, invested, managed, converted, exploited or to a third party transmits.

According to Art. 165, Para 5 of the Criminal Code: '*A component of property arises from a criminal act if the perpetrator of the criminal act has obtained it through the act or received it for its inspection, or if it embodies the value of the asset originally acquired or received*.'

Exploring the above, we can conclude that the Austrian definition for money laundering is: **the act of concealing or hiding any part of assets that result from an act, threatened with more than a year in prison or an offense pursuant to specific crimes, and veiling their origin, in particular by providing false information in legal transactions regarding the origin or the true nature of these property components, the property or other rights to them, the power of disposal over them, their transfer or where they are located**.

Prosecuted as money laundering are also the following actions: the intentional act of acquiring, storing, investing, managing, converting, exploiting, or transferring to a third-party goods that knowingly comes from an act of crime. Also punishable is the act of bringing (safekeeping, investing, managing, converting, exploiting, or transferring to a third party) assets of a criminal organization or a terrorist organization.

Comparison of the definitions

The aforementioned definitions consist of similar components and have the same purposes – to describe the wide circle of possible actions that one can intentionally perform, in order to hide the origin of assets, obtained by crime, and to be able to freely use them and sabotage the investigation of the initial crime, by which the assets were obtained.

However, the definitions are not the same. They use different terminology and some has wider impact than others. In the table below, there is comparison of the termins, incorporated in the definitions and conclusion for their scope of regulation.

Terminology for the subject of money laundering

1. Directive	**Property** (derived from criminal activity or from an act of participation in such an activity);
2. Germany	**Object** (derived from one of the unlawful acts);
3. France	**Property or income**, direct or indirect products of a felony or misdemeanor;
4. Italy	**Money, goods or other things of value**, deriving from an intentional crime;
5. England	**Proceeds of crime**;
6. Austria	**Assets** that result from an act, threatened with more than a year in prison or an offense pursuant to specific crimes.

Terminology of acts, by which money laundering can be performed

1. Directive	Intentional (and with knowledge that such property is derived from criminal activity or from an act of participation in such activity): - conversion or transfer of property; - concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property; - acquisition, possession or use of property; - participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred above.
2. Germany	- hiding an object, concealing its origin, or obstructing or endangering the investigation of its origin;
3. France	- false justification of the origin of the property or income; - assistance in investing, concealing or converting the direct or indirect products of a felony or misdemeanor.
4. Italy	- informed and intentional substitution or transfer, in such a way as to obstruct the identification of the criminal provenance.
5. England	- trying to disguise the illegal origin of proceeds of crime.

6. Austria	- concealing or hiding any part of assets that result from specific crime, veiling their origin;

2. RESEARCH OF MONEY LAUNDERING

2.1 IDENTIFICATIONS

2.1.1 Rules for identification of risks and high-risk clients and transactions.

Amongst the main obligations under the AML legislations, lays the requirement the obliged entities to create and accept Internal AML Rules, individual for each specific entity.

In Bulgaria this obligation is given by the **Measures against Money Laundering Act** (‘**MAMLA**’).

Under Art. 101 of MAMLA:

‘*The entities obliged under Art. 4 shall adopt internal rules for control and prevention of money laundering and financing of terrorism, which shall be applied effectively also to their branches and subsidiaries abroad.*’

REQUIREMENTS

There are strict legal requirements of the minimal content of the Internal rules. Therein the entities shall cover wide aspect of relevant information. The drafting of the Internal rules helps the entities to acknowledge better their AML legal obligations and to individualize and analyse the main risk. In the previous Bulgarian AML Act (in force since 1998 until 2018) such obligation for Internal rules was not included.

The necessity for compliance of the Internal rules with the National Risk Assessment helps the entities to develop deeper understanding of its content and match the rules and conclusions therein to their personal situation.

WHAT THE LAW SAYS

Under Art. 101, para 2 of MAMLA, the Internal rules shall contain:

1) Clear criteria for recognizing suspicious operations or transactions and clients:
2) The procedure for using technical means for prevention and disclosure money laundering and financing of terrorism;
3) An internal control system over the implementation of the obligations, established in this act, the Measures against Financing of Terrorism Act and the instruments on their implementation;

4) Possibility for performing review by internal audit, where the person under Art. 4 has established such, in which the rules, procedures and requirements are to be checked and assessed under this Paragraph;
5) Possibility for performing an independent audit, in which the rules, procedures and requirements under this Para. Are to be assessed, where this is appropriate in view to the size and nature of the economic activity of the person under Art. 4.
6) The internal system under Art. 42;
7) The internal system for risk assessment and defining the risk profile of the clients;
8) Proportional to the size and nature of the economic activity of the person under Art 4. Policies, control mechanisms and procedures for limitation and effective management of the risks of money laundering and financing terrorism, established at the EU level, at national level, as well as at the level of obliged subject;
9) Rules and organization for implementation of the obligations for clarifying the origin of the funds and the source of the property status;
10) The conditions and procedure for collecting, storing and disclosure of information;
11) Time intervals, during which the maintained data bases and clients' files are reviewed and updated in implementation of Art. 15 and 16, while observing the established and documented under Art. 98 risk level for the clients and business relations;
12) Distribution of the responsibility for application of the measures against money laundering and financing of terrorism in the branches of the person under Art. 4 and measures, including procedures for risk assessment in relation to branches and subsidiary companies in the conditions of Art. 7, if any;
13) The rules for organization and for operation of the specialized service under Art. 106, as well as the training rules of the employees in the specialized service;
14) The training rules for the remaining employees;
15) The distribution of the responsibility of the representatives and employees of the person under Art. 44, as well as to persons in a similar situation, engaged in his/her activity on other grounds for fulfilling the obligations, set out in this Act in the Act on Measures against Financing of Terrorism and in the instruments for their implementation, as well as contact information with the person under Art. 4 and with its responsible representatives and employees and persons in a similar position, engaged in its activity on other grounds, for the purposes of this Act, the Act on Measures against Financing Terrorism and their implementing instruments;
16) in proportion to the size and nature of the economic activity of the person under Art. 4 procedure for anonymous and independent submission of internal reports by employees or persons in a similar position, engaged in his activity on other grounds, for violations of this Act, the Act on Measures against the Financing of Terrorism and their implementing instruments, including alerts for existing suspicion for money laundering or terrorist financing;
17) The assessment under Art. 98, Para. 4;
18) Other rules, procedures and requirements according to the peculiarities of the activity of the person under Art. 4.

2.1.2 Identification of businesses, branches and industries with higher risk with respect to Money Laundering, e.g. financial institutions, crypto currencies

- **Financial Institutions**

Financial institutions, otherwise known as banking institutions, are corporations that provide services as intermediaries of financial markets. Broadly speaking, there are three major types of financial institutions:

- Depository institutions – deposit-taking institutions that accept and manage deposits and make loans, including banks, building societies, credit unions, trust companies, and mortgage loan companies;

- Contractual institutions – insurance companies and pension funds

- Investment institutions – investment banks, underwriters, brokerage firms.

Every Financial Institution should identify and analyze Money Laundering (ML)/Terrorist Financing risks (TF) present within the financial institution and design and effective implementation of policies and procedures that are commensurate with and that mitigate the identified risks to ensure sound ML/TF risk management.

Banks have been the largest institutions in the field of finance since the past. Considering that even a single local bank mediates thousands of financial transactions throughout the day, when we look at the world, millions of financial transactions are realized through banks every day. Criminal gangs need financial resources to survive and grow their gangs.

Criminal organizations try to launder the money in order to use the crime earnings they get from crimes. According to the announced data, criminals carry out 97% of money laundering activities through financial institutions. Considering that banks mediate millions of financial transactions during the day, banks are at great risk against financial crimes. For this reason, banks must identify the risks by fulfilling their AML obligations and must take precautions for them.

The most important element of effective AML / CFT programs is the risk-based approach. FATF, the European Union, and most local AML regulators agree with the implementation of a risk-based approach to AML / CFT. According to the risk-based approach, the risk level of each customer is different. In addition, countries have different risk levels. For this reason, the businesses have to determine the risks of the customer and apply control processes specific to these risks by taking a risk-based approach. Banks are obliged to perform a risk assessment with customer due diligence and know your customer procedures by applying a risk-based approach in customer account opening processes. Banks then have to control their customers' transactions with the control mechanisms they have developed in accordance with their risk levels.

Know Your Customer /KYC/ in Banking or Know Your Customer control is the process of identifying the customer identity of banks when opening new customers. At this stage, customer information is collected and the accuracy of the collected customer information is checked by banks. That is, banks have to make sure that customers and customer information

match. KYC process can be done with various methods such as identity card verification, face verification and invoice as proof of address.

KYC is the process of identification and verification of the identity of a client in which a series of controls are applied to avoid having commercial relations with people related to terrorism, corruption or money laundering, among others.

The KYC process consists in verifying that the client is actually who he says he is and giving him access to the services or products he needs. This verification is carried out through different methods, although not all comply with legal requirements.

The process takes place in such a way that the user who wants to become client of a company demonstrates with legal and binding evidence his identity. For this, methods such as Video Identification by streaming video and videoconferencing are used, in which the user shows and validates his identity documents, the authenticity of them, and their face, in addition to other biometric tests and security checks.

Know Your Customer process can be carried out both remotely online and in-person at a commercial office or store. When it is done remotely and online, or the process has been digitized, we talk about eKYC process.

Banking and financial industries are some of the most complex sectors in terms of customer relations. Banks and financial institutions constantly face a number of risks in relation to money laundering and terrorism financing.

Having this in mind, governments and authorities have set standards in 5AMLD and eIDAS rules to create a reliable framework where KYC processes are completely secure.

The KYC banking process is no different than the same one in other industries, but high-security standards required by legislation are different from those required in other sectors.

Video-streaming is becoming the global standard for identifications within the financial sector and it is being included and standardized by regulations and law. Client onboarding has changed from a long, expensive, bureaucratic process to an optimized, more secure and quick process. 3 weeks have turned into 3 minutes with the highest security standards from any electronic camera device.

The process requires the financial sector to adhere to its regulations worldwide, which implies that identification with selfies or images is not valid due to its low range of technical security, the weakness of electronic evidence and the lack of its integrity.

Therefore, the level of security provided by these types of solutions is low, far from the legally required security standards for formal customer identification according to the most demanding regulations in this area.

Customer Due Diligence in Banking

Customer due diligence (CDD) is the control process implemented by banks to identify potential money laundering and terrorist financing risks carried by customers. Although these procedures are not exactly the same all over the world, the goal is the same: to identify risks. After the Know Your Customer control process, the risk assessment of the customer is made with the correct customer information.

The customer's information is checked in the required databases in the region served by the bank. These databases generally consist of sanctions, PEP, banned and wanted lists. The people on these lists carry high risks for money laundering and terrorist financing. In addition, in the banks that provide global services, the nationality of the customer and the past financial transactions of the customer affect the risk level of the customer.

Our AML Screening and Monitoring tool automates banks' Customer Due Diligence control processes. Banks can automatically scan their customers in global comprehensive sanctions, PEP and adverse media data during customer onboarding and customer monitoring processes.

Transaction Screening Processes of Banks

Banks generally have a broad customer portfolio. In addition, the transactions mediated by banks are not limited to their own customers. One customer of the bank can make payments and transfer money to another bank's customer. An average-sized bank mediates thousands of money transfers throughout the day.

Banks are obliged to control the buyer and the sender in these money transfer transactions. Because if the bank mediates the payment sent to a banned or sanctioned person, this is a big crime. The consequences of the crimes caused by the uncontrolled reception of the receiver and the sender are very severe administrative and fines and banks lose their reputation. In today's technology, manual controls are a waste of time and are dysfunctional. Banks need an automated transaction screening tool to carry out customer transactions in accordance with AML regulations.

The Transaction Screening tool provides banks to control the receiver and sender in financial transactions in the global coverage AML database. Banks can automate the entire control process by integrating their own systems and transaction screening tool with the API. All AML screening takes place automatically against the background of the transactions performed by the bank. If the system catches a match, it alarms and stops the process. The scanning process takes place within seconds and the customer process is not delayed.

Suspicious Financial Transactions

Definition of Suspicious Financial Transactions

As already known, the Money Laundering Law uses the term "**Suspicious Financial Transaction**". The word "suspicious" has the connotation that such financial transaction is surely related to a criminal act so as to pose impediment to Suspicious Financial Transaction reporting.

Basically, referred to as "Suspicious Financial Transaction" is the transaction that is unusual or improper and is not always related to a certain criminal act. The term "suspicious transaction" in the anti-money laundering terminology was initially used by the Financial Action Task Force on Money Laundering (FATF) in the Forty Recommendations concerning the eradication of criminal acts of money laundering. In practice every state may use different terms. The term used is not only "suspicious transaction", but also other terms such as "unusual transaction". There is no standard characteristic of Suspicious Financial Transactions as it is influenced by variation and development of existing financial services and instruments. However, here are general characteristics of Suspicious Financial Transactions, which can be used as a reference, as follows:

a. Transactions having unclear economical and business target
b. Transactions conducted in relatively large amount cash and/or conducted repeatedly and unnaturally.
c. Transactions conducted differently from that of usually and normally conducted by the relevant customer.

If required, PJK can clarify or request the supporting document of the transactions conducted by the customer, to determine Suspicious Financial Transactions. In reporting Suspicious Financial Transactions, the suspected object is dominated by the transaction itself rather than the person or customer conducting the transaction.

The importance of identification of Suspicious Financial Transactions

In committing money laundering, the perpetrator does not normally spend or use the properties obtained from his/her criminal act directly, but he/she will first try to put such properties into the financial system through placement, layering or integration phases. With respect to the aforementioned matter, the identification of Suspicious Financial Transaction is one of the important activities to be conducted by PJK in producing quality report on Suspicious Financial Transaction. Such action is required to support the efforts of preventing and eradicating criminal acts of money laundering and terrorism funding as well as securing the financial system so that it will not be used for illegal purposes.

- **Elements and Indicators of Suspicious Financial Transactions**

Elements of Suspicious Financial Transactions

In accordance with Article 1 item 6 of the TPPU Law, a Suspicious Financial Transaction basically has the following elements:

a) Transaction deviating from:
   - the profile;
   - the characteristics; or
   - the usual transaction pattern of the relevant customer.

b) Transaction reasonably suspected to have been conducted with the purpose of evading the reporting that must be conducted by the relevant PJK.

c) Financial transaction conducted using fund alleged to be attributable to criminal acts.

If a financial transaction indicates one or more of the aforementioned elements, the relevant PJK must identify it as a Suspicious Financial Transaction and report it to the PPATK.

Indicators of Suspicious Financial Transactions

In identifying whether or not a financial transaction has one or more of the aforementioned elements, the relevant PJK can use the indicators of Suspicious Financial Transactions, which include, among other things:

a. Transactions

1) Cash

i. Cash transactions conducted in an unusual amount from that of usually conducted by the relevant customer.
ii. Transactions conducted in a relatively small amount but with high frequency (structuring).
iii. Transactions conducted by using several different individual names for the interest of a particular person (smurfing).
iv. The foreign currency exchange or purchase in a relatively large amount.
v. The purchase of travelers checks in cash in a relatively large amount.
vi. The purchase of several insurance products in cash in a short period time or at the same time with premium payment entirely in a large amount and followed by policy disbursement prior to due date.
vii. The purchase of securities by cash, transfer, or checks under other person's name.

2) Economically irrational transactions

i. Transactions having no conformity with the initial purpose of account opening.
ii. Transactions having no relationship with the business of the relevant qcustomer.
iii. Transaction amount and frequency are different from that of normally conducted by the customer.

3) Fund transfers

i. Fund transfers to and from high-risk offshore financial centers without any clear business purposes.
ii. Receipts of fund transfers in several phases and once accumulated the funds are subsequently transferred entirely to other account.
iii. Receipts and transfers of funds at the same or approximately the same amount and conducted in a relatively short period (pass-by).
iv. Fund payments for export import activities without complete documents.
v. Fund transfers from or to other high-risk countries.
vi. Fund transfers from or to other high-risk parties.
vii. Receipts/payments of funds made by using more than one (1) account, either in the same name or a different one.
viii. Fund transfers using the account of PJK's employee in an unusual amount.

b. Behaviors of the Customer

1) Unreasonable behaviors of the relevant customer when conducting a transaction (nervous, rushed, unconfident, etc.).
2) Customer/prospective customer gives false information with respect to his/her identity, sources of income or businesses.
3) Customer/prospective customer uses identification document, that is unreliable or alleged as fake such as different signature or photo.
4) Customer/prospective customer is unwilling or refusing to provide information/documents requested by the officials of the relevant PJK without any clear reasons.
5) Customer or his/her legal representative tries to persuade the officials of the relevant PJK in one way or another not to report his/her transaction as a Suspicious Financial Transaction.
6) Customer opens account for a short period.
7) Customer is unwilling to provide right information or immediately terminating business relationship or closing his/her account at the time the officials of the relevant PJK request information with respect to his/her transaction.

- **The Importance of Transaction Monitoring in Banking**

Only people in the sanction, PEP and adverse media database do not commit financial crime. Therefore, each customer carries a risk of financial crime for banks. For banks, any transaction they intermediate can be a financial crime. There are a lot of money laundering methods, and with the development of technology, these crime types increase even more. It is impossible for banks that mediate thousands of transactions during the day to manually control these transactions. In today's technology, transaction monitoring tools do this automatically.

Banks create various rules with AML Transaction Monitoring software and every transaction they mediate is controlled automatically based on these rules. Banks are the most audited institutions in this period when regulations and audits for AML increased. Our AML transaction monitoring software enables banks to perform transactions they mediate in accordance with AML regulations.

With our advanced features, banks can create dynamic rules and scenarios and test these rules before they go live with the sandbox test environment. With real-time alarm management, the AML department can instantly see the alarm level of all transactions and assign tasks to teammates related to these transactions. All logs are recorded and the bank can show these logs as evidence in possible audits. With customizable settings, banks make control processes more efficient and reduce AML false positives.

- **Independent AML Audits**

Independent AML audits enable banks to control the AML compliance program end-to-end. Although banks have their own AML departments, it is vital to control them with independent audits. Deficiencies detected by independent audits may perhaps protect banks from millions of dollars in fines and prevent reputation losses. According to the independent audit reports, banks compensate for the deficiencies in AML compliance programs and further develop the

AML program. Therefore, banks should have the AML program checked by performing an independent audit at 1 or 2-year intervals.

- **Crypto currencies**

What is crypto-asset?

Crypto-assets are a global phenomenon: they are created by private actors in various countries all over the world, they are cross-border in their application and infrastructure, and they are easily accessible, transferable, exchangeable and tradable from nearly anywhere in the world. To address the challenges, regulatory authorities will have to step in. In some countries legislators have already taken action or are planning to do so. These national initiatives are not necessarily aligned with each other, leading to regulatory arbitrage. To avoid regulatory arbitrage, rulemaking on crypto-assets should ideally take place at the European level, preferably in the execution of international standards. At the start of 2020, over 5 100 crypto-assets exist with a total market capitalisation exceeding EUR2200 billion. Both lawful and unlawful crypto-markets exist. Most legal activity in crypto-assets – and in particular in cryptocurrencies – takes place on crypto-exchanges. It relates mostly to the use of cryptocurrencies for speculative purposes.

The illegal activity includes, amongst others, the buying and selling of illegal goods or services online in darknet marketplaces, money laundering, evasion of capital controls, payments in ransomware attacks, and thefts. In this context, cryptocurrencies function mostly as a payment instrument. Remarkable is that almost half of all (yearly) transactions in Bitcoin can be linked to illegal activity. As the crypto-market is still dominated by Bitcoin, with a dominance in terms of total market capitalisation exceeding 63% (EUR140 billion), this is an important observation.

To address the ML/TF risks presented by cryptocurrencies - or, as the EU up until now referred to them, "virtual currencies" - the EU legislator included so-called "*custodian wallet providers*" and "*providers engaged in exchange services between virtual currencies and fiat currencies*" within the scope of the Anti-money laundering / Combating the financing of terrorism (AML/CFT) framework by defining them as obliged entities in AML Directive 5.

To bring the European AML/CFT framework up to speed with the current reality in the crypto-space, the EU could consider a number of regulatory actions:

Broaden the scope

A first regulatory action to consider is to broaden the scope of the definition of virtual currencies, for instance to include tokens.

Broaden the list of obliged entities

The list of obliged entities could be broadened. The following blind spots could be addressed:

- crypto-exchanges exchanging crypto into crypto;

• financial service providers who are active in the participation in and provision of financial services related to an issuer's offer and/or sale of a crypto-asset; and
• trading platforms, at least insofar they are centrally operated.

An interesting question is whether it would not also make sense to include issuers or offerors of crypto-assets into the list of obliged entities. Non-custodian wallet providers only provide the technical tools for others to work with and typically do not function as an intermediary so it does not make much sense to target them for AML/CFT purposes. The same holds true for coin inventors.

A different approach is warranted for miners. Nowadays, coins have emerged that do not always require big energy-consuming server farms to mine, but that can be mined running a few hardware rigs at home. As it stands, such rigs can be set up by anyone, even criminal actors. Regulators should be aware that by mining coins, directly or indirectly via front men, criminal actors can get access to clean cash. Newly mined coins are by definition "clean", so if someone (e.g. a bank) is willing to convert them into fiat currency or other crypto-assets, the resulting funds are also clean. A first regulatory step could be to try to map the use of this technique and subsequently, if it effectively proves an important blind spot, to consider appropriate counter measures.

In addition, and in view of the cross-border nature of crypto-assets and their misuse, the introduction of a European AML watchdog could have various benefits, especially if it is staffed with highly trained IT personnel capable of analysing the AML/CFT risks new technologies bring. It could help promote information-sharing, serve as a new knowledge pool, and provide a more independent approach to AML/CFT cases. When enhancing the regulatory framework with respect to criminal use of crypto-assets, the EU should be mindful to also enhance the investigative toolbox: to ensure compliance with the regulatory framework, law enforcement agencies must be able to detect infractions and subsequently sanction them.

2.1.3 Identification of transactions or instruments used for ML

There are three basic methods by which the criminal organizations and the terrorism financing entities provide cash flows to cover their sources and to integrate them into the economy, namely:

1. the use of the financial system through methods such as checks or wire transfers;
2. physical movement of cash - physical movement of cash using methods such as cash-carrying couriers and the smuggling import / export of large amounts of cash;
3. physical movement of good through the international trade system - movement of resources through methods such as false documentation and declaring goods and services subject to commercial transactions.

Each of the above involves the movement of huge amounts of funds and can function both locally and internationally.

Transactions

The international trade system is exposed to a wide range of risks and there are weaknesses that could be exploited by criminal organizations and terrorism financing entities.

The risks and weaknesses are result from the huge volume of trade flows that makes it impossible to take into account:

- individual transactions;
- the complexity associated with the use of multiple foreign exchange operations and the various mechanisms for financing commercial transactions;
- mixing legal and illegal funds;
- as well as the limited resources available to detect the dubious business transactions most customs services have.

The above gives the criminal organizations and the terrorism financing entities the opportunity to launder the incomes of crime and to provide funding to terrorist organizations at relatively low risk of detection. The international trade system is attractive to be used for money laundering because of:

- the huge volume of trade flows that conceals individual transactions and offers great opportunities for the criminal organizations to transfer value across interstate borders;
- the complexity associated with the (often numerous) foreign exchange transactions and the use of different financing mechanisms;
- the complexity that may result from the practice of mixing criminal assets with cash flows from legitimate businesses;
- limited use of verification and clearance procedures and customs data exchange programs between the Countries;
- the limited resources available at most customs offices for detection of illegal commercial transactions.

The movement of capitals connected with money laundering or the money laundering through commercial transactions, includes incomes from crimes, which are harder for tracking.

The main technics for money laundering through commercial transaction includes:

- over and under invoicing of goods and services;
- multiple invoicing for goods or services;
- delivery of more or less goods or services;
- false description of goods or services.

Over and under invoicing of goods and services.

This is one of the oldest technic of transferring funds across borders. Key element of this technique is the inaccurate presentation of the price of the goods or services in order to transfer additional value between the importer and the exporter.

By invoicing the goods or services at price lower than the market price, the exporter is able to transfer value to the importer, as the payment for the goods or services will be lower than the value which the importer receives when this goods or services will be sold on the free market.

by invoicing the goods or services at price higher than the market price, the exporter is able to receive value from the importer, since payment for the goods or services is higher than the value the importer will receive when this goods or services are sold on the free market.

Over and under invoicing of goods and services might have significant tax consequences. An exporter who increases the value of the goods shipped may be able to substantially increase the amount of the export tax credit he receives. An importer who is invoiced with a lower value of the received goods may be able to substantially reduce the amount of import duties (or customs duties) which are payable.

When more complex goods are being traded, the greater will be the difficulties that customs will experience in identifying cases of over or under invoicing and in correctly determining the amount of duty or tax.

Multiple invoicing for goods or services

This technic is expressed in issuing more than one invoice for the same international commercial transaction. By invoicing the same goods or services more than once, a person involved in money laundering or terrorist financing is able to justify multiple payments for a single delivery of goods or a single provision of services. The use of several different financial institutions is preferred in this method because it increase the level of complexity that accompanies such transactions.

In addition, even if multiple payments related to the same supply of goods or services are detected, there are a number of legitimate explanations for such situations, for examples: changes in payment terms, adjustments to previous payment instructions or late payment.

Delivery of more or less goods or services

This means overstatement or understatement of the quantity of the shipped goods or the provided services. The exporter may not deliver any goods, but simply negotiate in secret with the importer to ensure the routine processing of all shipping and customs documents related to this type of deliver (they are called “phantom deliveries”).

False description of goods or services

In this technic the money laundering person may inaccurately represent the quality or type of goods or services. The exporter can ship relatively cheap goods and instead to invoice them as a more expensive or completely different goods. This way they create a discrepancy between what is evident from the shipping and customs documents and what is actually delivered. The use of a false description may also apply to trade in services, such as financial consulting, market research and consultancy services.

New payment and development methods

The development of new payment methods (‘**NPM**’) creates new opportunities for using such technologies for money laundering and terrorism financing.

The NPM has evolved as a result of the market need for alternatives to traditional financial services. In some cases, this development is driven by the need for more convenient and secure ways to pay for online orders. In other cases, there is a desire to provide financial services for persons with limited access to traditional financial services.

The money laundering legislation requires from the obliged entities when establishing relationships with clients without their physical presence on the premises of the institution to apply equally effective identification procedures and standards for ongoing monitoring equivalent to the procedures for the customers which introduce themselves personal.

There must be specific and appropriate measures to reduction of the higher risk. Exemplary risk reduction measures can be:

- confirmation of the correctness of the submitted documents and requesting additional documents;
- confirmation of the identification from other oblige entity or from person obliged to apply the anti-money laundering measures in EU country;
- establishing a requirement that the first payment for the transaction should be made through an account opened in the name of the client at a Bulgarian bank, a branch of a foreign bank, licensed / licensed / by the BNB to operate in the country through a branch, or a bank from a country - member of the European Union.

The development of NPM by categories:

A. Development of the use of prepaid cards:

Prepaid cards can be divided into two categories - open-loop cards and closed-loop cards. The closed-loop card has a much more limited transferability, but that doesn't mean that the risk connected with them is necessary lower.

The prepaid cards can be an alternative to many traditional banking products and services such as debit or credit cards and travelers checks. Many prepaid cards allow for international payments. Such card products enable the customer not only to make payments, but also to receive payments from third parties, as well as to make cross-border transfers, e.g. by issuing multiple "paired" or "affiliate" cards to one client that can be transferred to users anywhere in the world. The cards give the holder access to real funds from the start cards through the global ATM network.

B. Development of online payment services

Online payment services can be provided by financial institutions and companies outside the financial sector. They can be linked with a bank account or used regardless from the bank account. Internet payment methods can be divided into three categories:

- online banking where credit institutions offer online access to traditional banking services based on a credit institution account on behalf of a customer;

- prepaid internet products where companies, which may not be credit institutions, allow their customers to send and receive funds through virtual, prepaid accounts available online;
- digital currencies, where customers typically buy units of digital currencies or precious metals that can be transferred between account holders of the same service or exchanged against real currencies and drawn.

The market for prepaid internet products has diversified and grown since 2006 in many parts of the world and the moment is one of the most used methods for payments. In recent years, there has been the emergence of electronic currencies, in which users exchange real for virtual currencies to make payments within the virtual world. Virtual currencies can be traded and converted into real currencies.

The online payment services are increasingly interconnected with other new and traditional payment services. Funds can now be transferred from/to a variety of payment methods involving cash transfer companies.

C. Development of mobile payment services

It is important to distinguish "mobile payments" based on individual bank or investment accounts for each client of a financial institution with adequate control and compliance with the money laundering and terrorism financing framework from services used independently from such accounts. The World Bank review four categories of mobile payment systems:

- mobile financial information services: Users can view their personal account information and general financial information, but cannot transact, so these services are considered low-risk;
- mobile banking and investment account services: Consumers can transact in the same way as Internet banking;
- mobile payment services: These allow non-bank and non-investment account holders to make payments via mobile phones;
- mobile money services: Their users can store real value funds on their mobile phones. They can use phone credits or call time as a payment method.

Risk assessment of the NPM

Like all financial services and products, the NPM can be used for money laundering and terrorism financing purposes. Unlike the cash operations, the NPM can provide additional clues for the identification of illegal activity by law enforcement. This is because an NPM transaction will always generate an electronic record. Even where complex customer verification measures are not implemented (for example, when the client remains anonymous), in some cases the electronic record may give law enforcement authorities at least minimal information such as an IP address.

The NPM are considered as a better option for money laundering and terrorism financing by criminals than the cash operations. This is specifically used in cases where NPM's are a

substitute for large-scale cash transactions or where the nature of the indirect contact in a commercial relationship facilitates the use of fraudulent or false identities.

According to FATF, the main risks for NPM are:

- Lack of credit risk: Funds used in NPM are mainly prepaid, which means that service providers may have little stimulus to obtain complete and accurate information for the client and the nature of the commercial relationships;
- Speed of the transactions: Transactions carried out with NPM's allow much faster execution of operations than the traditional channels. This can complicate the monitoring and the efforts to freeze the funds;
- The indirect contact in the commercial relationships: Many NPM vendors carry out their business relationships and transactions through indirect contact with the customer, which increases the risk of fraud and the opportunity for customers to present themselves as someone else.

Risk management measures

A. Complex check of the customer

The prepaid cards can allow customer anonymity while maintaining a high degree of functionality. Prepaid cards can also be easily provided to anonymous third parties, which in some cases can be assimilated to the term "beneficial owner". This underscores the crucial importance of identifying the original account holder or cardholder to whom a product is linked.

It is always possible to use a payment card (including traditional debit and credit cards) together with a third party, which remains anonymous to the institution that issued the card. In this cases, the initial identification made by the institution will be the starting point for monitoring and subsequently investigating any illegal activity.

For many NPM providers, customer contact is often minimal or indirect. This increases the risk of fraudulent use of the product or the use of the product by third parties for illegal purposes. The absence of direct contact is particularly prevalent among online payment service providers, who typically conduct most of their online business activities.

The most online payment service providers require the names of their customers, but in order to limit the risk, a form of customer verification should also be included.

B. Data storage

The obliged entities are obliged to keep the date for the performed transactions and operation for a period of 5 years. The data must be sufficient to serve as evidence of a criminal proceedings and case.

C. Financing methods

NPM can be funded differently, including anonymously through cash, money orders or transfers of funds from other anonymous NPM products. The anonymous financing methods can lead to a lack of trace or insufficiency in the transactions performed and the origin of the funds. In this case, the client's due diligence obligations should be strictly enforced and the employee trainings in the area of combating money laundering and terrorism financing should be mandatory.

D. Geographic boundaries

The greater the geographical scope of the NPM product, the higher the risk of money laundering and terrorism financing. The cross-border functionality of the services makes it more attractive to money launderers and also allows payment service providers to pursue their activities from jurisdictions that may not be subject to adequate regulations and monitoring of the money laundering.

E. On use restrictions

On use restriction on NPM products may vary by product and by service provider. NPM products with limited functionality are less exposed to money laundering and terrorism financing than those that allow customers to use the product more widely.

The standards used for prepaid card payments are largely identical to those for regular debit or credit card payments, making them a payment method for almost anywhere, including from online stores. The payment services that are accepted by most local and foreign merchants are more attractive to money launderers than those that allow funds to be spent on a limited range of retail outlets.

Some services for payment through internet and services for mobile payment intend to ease payments from natural persons to legal persons only for transactions and shopping, which lower the risk of money laundering and terrorism financing. However, when such payments are used for criminal purposes, the risk of money laundering and terrorism financing is still high.

Cash withdrawal can be done with open-loop prepaid card through ATM networks. The easy access to cash combined with the fact that prepaid cards are much easier to transport allows them to be used in ML schemes.

When cash is used as a method of financing, it is usually also possible to withdraw cash from a mobile payment account. Not only does this increase the risk of ML and FT, but it can also create additional challenges for the mobile payment service provider (for example, through agents).

Some online payment and mobile payment service providers also offer prepaid card charging, allowing their customers to withdraw cash via ATM's worldwide distribution network.

F. Complex services

When several parties are involved in the implementation of the joint payment service, the NPM are at higher risk. The number of this parties generates potential risks for loss of information. This can be worse if important services are outsourced to potentially unregulated third parties without clear accountability and oversight criteria, or located abroad.

Providers often use agents not only to cash in and withdraw cash, but also to establish new customer relationships. In these cases, the НПМ provider will be responsible for any failure by the agent of an obligation arising from the ML and FT legislation.

Use the nature of NPM accounts as payment methods without direct contact

Many of the NPM rely on a business model where direct visual contact with the customer is minimal or completely absent and this ease the abuse with money laundering.

In many cases, the NPM products have been used to launder illegal funds obtained through fraud such as identity theft, bank account theft, or credit/debit cards through computer hacking and phishing methods. Because bank accounts and credit/debit cards are in the name of legal customers, criminal clients use them as reference accounts to power prepaid cards or accounts in online payment systems. In such cases, NPM providers are unable to detect that the transactions are not actually ordered by their legal customers, or to identify any suspicious activity.

In other cases, stolen or fake identity is used to create NPM accounts, which are also used as transit accounts for the laundering of proceeds of crime or for the simultaneous pursuit of criminal activities and money laundering.

Prepaid cards and NPM accounts are in most cases used as transit accounts. Once the fund from crimes have been transferred to these accounts, the criminals or their accomplices withdraw money from an ATM device or spend it to buy goods. This often happens online.

Collaboration with NPM providers or their employees

There have been a number of cases where prepaid card and payment service providers or their employees are controlled by criminals and voluntarily or negligently support money laundering and terrorism financing activities. In such cases, the restrictions on admission to the market as existing control are not fulfilled or are not applicable to the company concerned under that jurisdiction.

Cross-border transfer of prepaid cards

Another identified risk of prepaid card abuse is the replacement of cross-border cash transfers with cross-border physical transfer of prepaid cards.

Indicators for the recognition of suspicious operations

In the case of indicators of doubtful activity, the actual use of NPM products and services is different from the expected one and there is no economic basis. Indicators should therefore not be administered instinctively but according to product characteristics.

Indicators for NPM:

- discrepancies between the information provided by the client and the information established by the monitoring systems;
- individuals holding an unusual number of NPM accounts with the same provider;
- a large and diverse source of funds (i.e. bank transfers, credit cards and cash received from different locations) used to charge the same NPM account/accounts;
- multiple linked accounts from banks in different cities that are used to charge the same NPM account;
- the supply or financing of an account is always made by a third part;
- multiple cash transfers below the threshold for declaring made on the same prepaid card/cards by the same individual/individuals;
- numerous financial activities by third parties on an NPM account, followed by an immediate transfer of funds to an unrelated bank account/accounts;
- multiple power supplies or financing the same bills, followed by quick withdrawals through ATMs for a short period of time;
- multiple cash withdrawals performed on different ATMs;
- NPM account used only for withdrawals and not for purchases through POS terminals or the Internet.

Specific indicators of suspected complicity of prepaid card providers:

- a large number of bank accounts held by the same prepaid card company (sometimes in different countries), apparently used as transit accounts;
- prepaid card company based in one country but with accounts in other countries;
- incoming and outgoing cash flows between different prepaid card companies' bank accounts based in different countries;
- the volume and frequency of cash transactions (sometimes structured below the reporting threshold) performed by the owner of a prepaid card company have no logical economic explanation.

Trends identified in the use of new technologies in money laundering schemes that could lead to anonymity

These trends are related mainly to the usage of different internet banking systems, payments on micro-accounts and virtual POS terminals, as well as schemes related to money laundering received through internet scams. The latter are known as "hacker attacks". Among them are virus infections, phishing scams and others.

The increasing use of internet banking systems is typical which commercial banks provide to their customers. Real-time transfers can be made from different geographical locations and the response time of banks is limited to compliance of their obligations, which are expressed in the

submission of suspicious reports operations. This type of service is preferred for money laundering. The recent information technologies allow concealment of IP addresses and the locations from where the bank accounts are handled. There are several main trends in money laundering schemes obtained through internet fraud:

- **Trend № 1:**

Hacker attacks are carried out on the accounts of foreign individuals opened in foreign banks. Subsequently, the funds are transferred to the accounts of a foreign legal entity that does not operate on the territory of Bulgaria. Through Internet sites, this legal entity offers for a fee / commission to Bulgarian individuals to receive a certain amount on their accounts, which they then withdraw at the cash register. The amounts are small - around several thousand euros. Bulgarian citizens either do not know about the criminal origin of the funds or are involved in the scheme for laundering the funds received. The latter are relied on for a longer period of time and they can receive several transfers within a short period. People who do not suspect that the amounts are of criminal origin usually receive no more than two or three transfers. After withdrawing the amounts at the cash desk, the person keeps the pre-determined commission and sends the rest through a system of money transfers.

Usually the accounts of Bulgarian individuals are certified with transfers, which are sent in files such as SEPA / Single Euro Payment Area - so bank customers can make transfers to beneficiaries' accounts in SEPA using the same bank account and the same payment instruments, standards and infrastructure. Basically, SEPA-compliant files combine a number of transfer operations that the receiving bank must accept in its entirety or reject in its entirety as well. The practice of SAD FR - SANS shows that the above scheme could be developed by complicating it in several directions:

Bulgarian citizens who are familiar with the scheme and the probable criminal origin of the funds could introduce another additional unit, which would aim to make it difficult to establish the origin of the funds. The introduction of such a unit is expressed in the arbitrary choice of persons (through physical contact with the same, for example on the street in front of a bank branch), where they are offered to open a bank account against a commission, to which they can receive a one-time transfer, which they can withdraw and hand over to the person who has made contact with them.

Introduction of the so-called “mules” of the second level, to which the funds should be transferred after their withdrawal to the cash register and subsequently these “mules” should send the funds via a system of money transfers abroad.

- **Trend № 2:**

The use of virtual POS terminals is associated with payments in connection with Internet commerce and credit card payments. The accepting bank manages and maintains the merchant's account to which funds due from the persons who have purchased the goods (the so-called cardholders) are transferred. The card issuing bank manages the cardholder's accounts, and the settlement bank transfers funds between the above-mentioned banking institutions.

The accepting bank issues a permit to the merchant to use a virtual POS terminal in connection with the electronic service provided by him or the traded goods. When making payments through virtual POS terminals, several steps are performed. First, this is the authorization, which is a confirmation of payment by the cardholder. It is in case of unregulated access to the payer's card that an invalid authorization is performed. Other processes that may be affected are clearing and the so-called "capture" process. This leads to settlement (after mandatory clearing), which is based on fraud.

Thus, schemes are built in which a company opens virtual POS terminals for making payments in connection with the online offering of goods or services. After the opening of these terminals, funds from multiple card accounts began to arrive. Subsequently, it turned out that they were not recognized by the cardholders. After receipt of the funds, they are withdrawn at the cash desk by a proxy or transferred via internet banking to a current account of the company. Subsequently, banking operations are carried out to break up and consolidate the amounts. Ultimately, the funds are usually transferred to the accounts of foreign legal entities - most often registered in offshore areas.

- **Trend № 3:**

Internet banking systems are often used in a variety of money laundering schemes. They allow easy access to the bank accounts of individuals. In the country, when building money laundering schemes, internet banking is used as an accompanying element, which will further complicate the tracing of the source and origin of funds.

2.1.4 Identification of online / gambling and bitcoin transactions used for ML

Virtual currency is a digital representation of value that can be digitally traded and functions as:

- a medium of exchange;
- a unit of account;
- a store of value.

It doesn't have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from fiat currency (a.k.a. "real currency," "real money," or "national currency"), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status. The virtual currencies also can be either convertible or non-convertible. Convertible (or open) virtual currency has an equivalent value in real currency and can be exchanged back-and-forth for real currency.9 Examples include: Bitcoin; e-Gold (defunct); Liberty Reserve (defunct);

Second Life Linden Dollars; and WebMoney. Non-convertible (or closed) virtual currency is intended to be specific to a particular virtual domain or world, such as a Massively Multiplayer Online Role-Playing Game (MMORPG) and under the rules governing its use, cannot be exchanged for fiat currency. There are several potential risks related to the convertible ones.

Convertible virtual currencies that can be exchanged for real money or other virtual currencies are potentially vulnerable to money laundering and terrorist financing abuse for many of the reasons. First, they may allow greater anonymity than traditional non-cash payment methods. Virtual currency systems can be traded on the Internet, are generally characterised by non-face-to-face customer relationships, and may permit anonymous funding (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source). They may also permit anonymous transfers, if sender and recipient are not adequately identified.

Decentralised systems are particularly vulnerable to anonymity risks. For example, by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity. There is no central oversight body, and no AML software currently available to monitor and identify suspicious transaction patterns. Law enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes (although authorities can target individual exchangers for client information that the exchanger may collect). It thus offers a level of potential anonymity impossible with traditional credit and debit cards or older online payment systems, such as PayPal.

Virtual currency's global reach likewise increases its potential AML risks. Virtual currency systems can be accessed via the Internet (including via mobile phones) and can be used to make cross-border payments and funds transfers. In addition, virtual currencies commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments. This segmentation of services means that responsibility for AML compliance and supervision/enforcement may be unclear. Moreover, customer and transaction records may be held by different entities, often in different jurisdictions, making it more difficult for law enforcement and regulators to access them. This problem is exacerbated by the rapidly evolving nature of decentralised virtual currency technology and business models, including the changing number and types/roles of participants providing services in virtual currency payments systems. And importantly, components of a virtual currency system may be located in jurisdictions that do not have adequate AML/CFT controls. Centralised virtual currency systems could be complicit in money laundering and could deliberately seek out jurisdictions with weak AML/CFT regimes. Decentralised convertible virtual currencies allowing anonymous person-to-person transactions may seem to exist in a digital universe entirely outside the reach of any particular country.

- **Money laundering with bitcoin**

Money laundering costs the global economy between $ 800 and $ 2 trillion a year, according to a UN report. This amounts to 2% -5% of the world's gross domestic product. Today, more than 90% of money laundering still goes undetected. However, the development of technology has led to new and faster tools. Criminals use these achievements to continue to launder money. At the same time, government agencies and fintech companies use technology to identify the attributes of transactions and help detect fraud.

Bitcoin is the most popular digital asset used today. In the media, bitcoin is often linked to the infamous Silk Road - the first online modern darknet market - where online users would anonymously buy items such as weapons and illegal drugs. In 2013, the US Federal Bureau of Investigation ruled out the first iteration of the market.

- **AML penalties in 2019**

2019 was a record year in terms of the number of fines imposed: Authorities imposed 58 sanctions on AML totaling $ 8.14 billion, twice the amount imposed in 2018, with 29 fines totaling $ 4.27 billion Dollars. The most aggressive were US regulators, who imposed 25 fines totaling $ 2.29 billion, followed by the United Kingdom with 12 fines totaling $ 388.4 million, according to a recent report.

Two-thirds of the sanctions against AML were imposed on banks, while approximately 17% were imposed on organizations in the gambling, gambling and cryptocurrency sectors. These industries are subject to stricter control by regulators, as they are common channels for money laundering.

- **Stages of money laundering**

Criminals paid in cryptocurrency must receive their final payment in cash. This requires obscuring where their funds come from. Unfortunately, several sophisticated services and tools help criminals do this. There is an example of the money laundering process:

1. Setting as a starting point: cash flow from its source. The money is put into circulation within the existing monetary system through intermediaries such as financial institutions, casinos, shops and currency exchange. Examples of these activities include currency smuggling from the state, complicity of banks, currency exchange, purchase of assets, etc.

2. Layering. In the second stage, the goal is to make it challenging to uncover money laundering. To this end, criminals must accumulate their costs and make it difficult to identify traces of illicit money. This usually happens by converting money into monetary instruments or buying assets with illegal funds to resell them.

3. Integration. This is the last stage of money laundering, when the laundered money are returned to the economy through the banking system and is therefore considered "clean". The methods include, but are not limited to, real estate transactions, front companies, foreign banks and counterfeit invoices.

- **Points of contact between bitcoin and gambling**

Today we can make all kinds of payments with our bitcoin wallet, including playing in online casino. In 2011 the new cryptocurrency (Bitcoin) is used for the first time in the field of online gambling. Then a poker game site appeared, where the payment was made entirely with bitcoin.

In April 2012, another important event in the history of cryptocurrency took place. Erik Voorhees, a well-known follower of bitcoin technology, launched the Satoshi Dice website, which still operates successfully today. Soon after its release, Satoshi Dice became the place where more than half of the world's bitcoin transactions take place. A year later, Voorhees decided to sell his creation to an unknown buyer.

In June 2013, the Just Dice project was born - the first crowdfunded crypto casino. Just a month later, Just Dice is now a serious competitor to Satoshi Dice. However, difficult times are coming for the casino, when human error leads to the loss of more than 1,300 bitcoins. Then we started talking more seriously about the weaknesses that were present in bitcoin gambling at that time.

Today, blockchain technology continues to revolutionize many industries, including gambling. It is becoming easier for players to pay with cryptocurrency, which is now possible through electronic wallets such as Skrill and Neteller. The number of people who are tempted by the anonymity and security that blockchain technology guarantees to consumers is also increasing.

- **General risks in casinos**

By definition, casinos are non-financial institutions. As part of its business casinos offer gambling for entertainment, but also carry out various financial activities that are similar to those in financial institutions, which puts them at risk of money laundering. Most, if not all, casinos carry out financial activities similar to those of financial institutions, including: accepting money into an account, conducting currency exchange, carrying out money transfers, foreign currency exchange; valuables storage services; devices for withdrawing cash from debit cards, cashing checks, safes, etc. In many cases, these financial services are offered around the clock.

The variety, frequency and volume of transactions make the casino sector particularly vulnerable to money laundering. Casinos are by nature a money-intensive business and most transactions are made in cash. During a single visit to the casino the customer can undertake one or many cache or electronic transactions or in stages "Entry", or at the stage "exit" from the game. It is this routine exchange of money cash for chips, tiles, TITO tickets and certified checks, as well as the execution of electronic transactions to and from deposit accounts in casinos, in casinos located in other countries, and the movement of funds to and from the financial sector is making casinos an attractive target for those who trying to launder money.

- **Methods and techniques for money laundering in casinos**

1. Use of valuable casino tools (cash/chips/TITO tickets/credits for gaming machines/cash orders/casino checks/gift certificates/vouchers for the purchase of chips/casino prize cards).

Money launderers usually buy chips through cash or through your casino account. Chips purchased on account can use a voucher for buying chips or other similar valuable instrument. Payment after this is done by check, warrant or transfer from the casino account. This method can become even more opaque if casino chains are used, where chips purchased with illegal cash are converted into credit and transferred to another a country where the casino chain has a branch; the loan then turns into check in the second casino. Money launderers can hold the chips for a while, or use them chips to gamble in the hope of making credible winnings, or by later they replace the chips for cash/check/transfer.

The money launderers can buy chips from other money launderers or from permanent ones that have nothing to do with them casino visitors with a "pure" reputation. This is done at a price higher than the face value of the chip and is sometimes called counterfeiting.

The money launderers can keep casino chips to use as a medium of exchange for the purchase of drugs and other illicit goods. The presence of chips from a drug deal can also contribute to an alibi for the predicate offense. The recipient of the chips will then turn them into cash at the casino.

Chips intended to be used as a means of payment may be transported across the border and exchanged for illegal payment activity, then returned again by third parties and cashed into the casino that is theirs issued in amounts below the stated in the declaration. In most countries, casino chips are not perceived as monetary instruments and therefore for their transfer no customs declaration is required.

**** Indicators for money launderers using currency casino tools:***

- customers who regularly insert a large number of banknotes into gaming machines that have a high payout rate and do not play a "maximum bet" to limit the possibility of significant losses or gains, thus accumulating gaming credits with minimal bets;

- two or more customers who often bet against each other in even games;

- buying and cashing chips with little or no betting;

- requesting or withdrawing many checks from an account;

- large volume of transactions for a short period;

- large number of chip casings in one day and etc.

2. Structuring.

Structuring or "smurfing" involves the fragmentation of large sums cash on a number of smaller transactions in order to minimize suspicions and exceed the mandatory disclosure threshold. The usual structuring methods include:

- regular deposit or transfer of similar amounts of cash that are below threshold for mandatory disclosure of the country;

- the use of third parties to carry out transactions with the use on one or many accounts;

- the use of checks from different financial institutions or branches of financial institutions for "redemption", as long as the amount of each check is below mandatory disclosure threshold and etc.

3. Refining - exchange of low denomination currency against high denomination currency value.

4. Usage a casino account for consolidation - laundries deposit small banknotes in their casino accounts, and withdraw money with a higher face value.

Casino accounts provide criminal elements with further opportunities to launder money from criminal proceeds. Many casinos offer deposit accounts and credit lines with fewer research requirements and customer verification than financial institutions. The frequent movement of funds between financial institutions and casinos, or between casino accounts, open in various casinos, may be vulnerable to money laundering. Many casinos offer personal safes, especially to VIP / "high-turnover" customers.

Some casinos allow customers to cash different types of checks and use the proceeds for bets. Checks can be signed to the bearer by the recipient of the check. In the present cases, the proceeds of illegal activity were initially used to withdraw these checks in order to avoid arousing suspicion. in the casino. The accounts are deposited by bank transfer or bank check, then cashed or transferred to other accounts after minimal or no gambling activity. The cashed funds are placed in safes or kept in the form of security markers and then cashed.

Many casinos offer safes to regular customers, especially to "high-turnover" customers in VIP lounges. They pose a risk due to the lack of transparency regarding the use of these safes and the possibility to be third party access to safes, using a password or key to facilitate banking operations. Very few countries control casino safes. Indicators for money laundering using casino accounts are:

- frequent deposit of cash, checks, bank checks, bank transfers in current accounts;

- withdrawal of funds from an account soon after their deposit;

- transferred money from a casino account to a charity fund;

- requests for opening casino accounts by prominent political figures (PEPs);

5. Profits.

Using illegal means of betting - this is the easiest method for raffling illegal funds, hoping to accumulate alimony profit check. One way to do this is with gaming machines or other games with low bets and a higher profit / loss ratio. Then the money launderer receives a casino check for the full amount of the remaining credit, plus the accumulated jackpot.

Redeeming profits from legitimate customers - this is another method used in the gambling sector. Money launderers offer customers cash as a premium over the amount of their profits. This is done with customers who win the jackpot from gaming machines, or collect a large amount of chips from winnings on games at the table, or customers who win from other types of bets offered by some casinos such as electronic lottery, horse racing and sports betting.

Indicators for money laundering through profits are:

- frequent jackpot claims;

- frequent deposits of winning checks from gambling, followed by the immediate withdrawal of cash;

- customers who watch/hang around betting points but do not participate in the game;

- customers claiming large payouts from gaming machines;

- cash winnings in various combinations of chips, checks and cash.

6. Currency exchange.

Given the popularity of gambling tourism and the desire of customers to travel to legitimate casinos, most of them offer services related to the exchange of currency.

Exchange of large amounts of foreign currency - money launderers can use large, one-time or frequent exchanges of foreign currency or deposits in foreign currency. This may not seem suspicious in countries with large numbers of foreign players.

Reported cases show that the criminal elements associated with the distribution and drug delivery, use the currency exchange services of casinos to transfer their criminal proceeds from one currency to another and change its original appearance.

Individuals and groups will also use structuring methods to exchange currencies without triggering reports to exceed the mandatory reporting threshold. They will use different casinos and after exchanging currencies, they will meet again to collect the total amount.

The game in the casino is made in foreign currency - in some countries with insufficient control, customers can buy chips directly in foreign currency (for example in Nepal with US dollars and Indian rupees). Some of the indicators for money laundering with currency exchange are:

- bank withdrawals / checks redeemed in foreign currency (euro, dollars);

- drastic or rapid increase in the volume and frequency of currency exchange transactions for ordinary account holders;

- currency exchange for no good reason;

- currency exchange related to the conversion of low denomination banknotes into high denomination banknotes;

7. Employee participation.

Employee involvement is another method that uses third parties to facilitate money laundering. Individual employees or organized groups, consisting of employees from different departments, conspire with customers to enable money laundering transactions to go unnoticed. Methods include:

- failure to complete suspicious transaction report or overrun reports the allowable transaction threshold;

- destruction of documents / transaction reports related to customer verification or reporting processes;

- counterfeiting customer ratings and other gambling rankings to justify the accumulation of casino chips/gaming machine credits;

Some countries have increased the level of vulnerability to include suppliers of gambling equipment and machinery, as well as suppliers of goods can potentially affect the integrity of the operation. Big contracts for delivery may be a way of using the operation with criminal intent (for example, through corrupt purchases and reduced delivery of contracted goods). Criminals will try to use gambling facilities and related computer systems to commit theft and laundering of money in the casino. There are some employee participation indicators:

- contacts between regular customers with employees outside the casino;

- the estimated profits do not match the registered profits;

- drastic or rapid increase in the volume and frequency of monetary transactions for regular account holders;

- casino account transactions made by persons other than the account holder;

- third parties are present in all transactions but do actually participate in no transaction;

- using money transfer companies to transfer funds across borders;

8. Credit cards/debit cards.

Money laundering from stolen credit cards - in some countries casinos allow customers to buy credit card chips. In cases when the cards are not stolen or fraudulently, the rest of the credit card is paid by the cardholder of the bank by illegal means.

Credit cards - the use of credit cards by criminal elements allows authorities to track money faster.

Debit cards - another monetary instrument used to commit fraud and money laundering. Criminals enter a casino and use their debit cards to withdraw the maximum standard amount at the casino for the day and buy casino chips. Objects or do not risk any funds, or bet very little. Then the objects are usually cashed the chips. In such cases, the records are handed over to a partner to play. Sometimes all the money is at stake. The main operators quickly noticed this trend and put in place risk control mechanisms to limit the initial debit card transaction to much lower levels for initial transactions in high-risk situations.

There are some indicators for money laundering via using debit or credit cards:

- buying casino chips with a credit or debit card;

- purchase and redemption of casino chips/plates without any gambling activity;

- usage of stolen or fraudulently acquired credit cards;

- usage of different credit/debit cards to purchase casino chips;

- usage of third parties to buy credit/debit card chips;

- structuring debit card transactions;

- carrying out debit card transactions up to the maximum limit.

9. False documents.

As with financial institutions, money launderers use false documents to disguise the origin of criminal proceeds and to protect the identities of those who launder the proceeds.

False identity documents - often used in operations in casinos, for opening casino accounts, undertaking gambling operations and buying out profits. There are some indicators for money laundering with using false documents and counterfeit money:

- links between different accounts under different names;

- purchase chips or make cash transactions immediately then leaving the casino;

- transfer of funds to third party accounts;

- obstacles to customer verification, such as refusals, false documents, one-time bets, tours;

- contradictory identity information presented;

- refusal to present an identity document/fake identity document or fake social security number;

- use of a false or more than one social security number;

- refusal to present the requested identity documents.

2.1.5 Identification of cash flows and jurisdictions for channeling of such flows

Huge sums are transferred from developing countries every year. These are illegal cash flows that take away resources from developing countries that could be used to fund much-needed public services, from security and justice to basic social services such as health and education, weakening their financial systems and economic potential.

Although such practices are found in all countries - and are harmful everywhere - the social and economic impact on developing countries is more serious given their smaller resource base and markets. Estimates vary considerably and are highly debated, but there is a general consensus that illicit cash flows are likely to exceed aid flows and investment volumes.

The most immediate impact of illicit cash flows is the reduction of domestic costs and investments, both public and private. That means fewer hospitals and schools, fewer roads and bridges. This also means fewer jobs. Many of the activities that generate illegal funds are criminal and while financial crimes such as money laundering, corruption and tax evasion are harmful to all countries, the effects on developing countries are particularly corrosive. For example, corruption diverts public money from public use to private consumption. Private consumption has much lower positive multiplier effects than public spending on social services such as health and education. Proceeds from corruption or criminal activity will usually be spent on the consumption of items such as luxury vehicles or invested in real estate, art or precious metals.

Money laundering is also detrimental to the financial sector: a functioning financial sector depends on the overall reputation for integrity that money laundering undermines. In this way, money laundering can damage long-term economic growth by harming the well-being of entire economies.

- ***Identification of illicit financial flows (or cash flows).***

There are different definitions of illicit financial flows. For example, illicit cash flows are known as a form of illegal that occurs when money is illegally earned, transferred, or spent. This money is intended to disappear from any record in the country of origin, and earnings on the stock of illicit cash flows outside a country generally do not return to the country of origin. They are essentially combined by methods, practices and crimes that aim to transfer financial capital from a country in violation of national or international law. The illicit cash flows generally involve the following practices: money laundering, bribery by international companies and tax evasion, trade mispricing.

These categories do not reveal the source or origin of the flows. They may have arisen from illegal or corrupt practices such as smuggling or counterfeiting; or the source of funds may be legal, but their transfer may be illegal, such as in the case of tax evasion by individuals and companies. Their purpose is not revealed. They can be used in other illegal activities, such as terrorist financing or bribery, or for the legal consumption of goods.

Flows range from transferring funds from private individuals to private accounts abroad without paying taxes to complex schemes involving criminal networks that create multi-layered structures with many jurisdictions to hide property.

The responsibility for tackling illegal flows is shared between developing and developed countries. It is widely recognized that developing countries must continue to build effective and accountable institutions to tackle illegal flows.

- ***Money laundering.***

Illegal cash flows often leave developing countries through the commercial financial system. Through this system, funds are laundered in order to conceal their origin. Money laundering

and terrorist financing regimes are effective tools to prevent the holding, receipt, transfer and management of illicit funds by large banks and financial centers.

Anti-money laundering regimes in OECD countries have improved since the first set of recommendations was set up in 2003, but not evenly. On average, compliance with OECD countries' recommendations of the central FATF is low. Twenty-seven of the 34 OECD countries maintain or require insufficient information on the beneficiary for legal entities, and no country fully complies with the recommendations for a property beneficiary for legal arrangements.

- ***Tax evasion.***

Combating international tax evasion is important because it is a major source of illicit financial flows from developing countries. Since 2000, the number of information exchange agreements between OECD countries and developing countries has been steadily increasing (to approximately 1300). Although most of the agreements signed in 2005 meet the standards of the Global Forum on Transparency and Information Exchange for tax purposes, there is room for improvement. Automatic exchange of information can be a powerful tool in this regard, deterring tax evasion and increasing the amount of taxes paid voluntarily. While automatic information exchange is becoming increasingly recognized for its effectiveness, it remains the exception. The tax systems of developing countries suffer from weak capacity and corruption and therefore often do not have the capacity to engage effectively in the exchange of information. Strengthening institutions and systems to prevent tax evasion is a priority.

- ***Jurisdictions channeling cash flows.***

Tracking and prosecuting illicit cash flow is complex.

A multi-legal and multidisciplinary approach is required. There is a need of lawyers, real estate experts, accountants who are also forensic scientists, bankers. There are a number of disciplines that have to work together.

The countries build their own institutions and jurisdictions to counter money laundering and cash flow control. These bodies are law enforcement, control, supervisory, specialized bodies for the establishment and confiscation of property acquired through criminal activity. Specialized units have also been set up at the main institutions for combating crime. An important challenge for countries is the insufficient human resources and the unsatisfactory level of administrative capacity.

There are formally developed instructions for inter-institutional cooperation and interaction. The cross-border nature of money laundering calls for international cooperation and the exchange of information. There are established bodies that monitor the process and develop effective solutions.

These bodies receive information and analysis from various sources such as state institutions, public and non-governmental organizations. It also compares the information and requires additional specialized analyzes of the environment in which the processes of generating

criminal means and their legalization take place. Their duty is to create and disseminate information about the money laundering process, to subject the regulatory framework to constant analysis and to assess the entire structure of countering and investigating money laundering and channeling cash flows.

There are employees who are responsible for the introduction of measures and requirements against money laundering in individual companies and organizations is one of the most important positions in the whole system of struggle with money laundering. Specialized employees have a great responsibility to combat money laundering. It is up to them to determine whether the information or other elements of the customer's data can give rise to suspicion of money laundering. They review the information of all transactions made by the client and assess whether
there is reason to report. Therefore, they must occupy a high enough position in the hierarchy of the company to be able to easily exercise their powers and impose the requirements to combat money laundering.

The main elements for the effective functioning of a specialized anti - money laundering service
money are providing appropriate training for employees, creating staff environment and conditions to facilitate rapid reporting of suspicious transactions and clients from each of the employees in the company, establishment of an organized system for collecting information and critical acquaintance and verification of the reports of the employees of the specialized department for counteracting money laundering.

Specialized employees must have information about customers and their activities, i.e. have full access to the information collected in consequence of the client's knowledge procedures. Among their responsibilities are the following:

- to prepare, at least once a year, a report to the management of the company, which describes the successes and failures in implementing the regime to combat money laundering;
- to provide feedback to the authorities and the regulator;
- to prepare reports on suspicious activities and clients, in accordance with the legal requirements for the manner and time in which they must be submitted;
- to observe the risky approach for counteracting money laundering;
- to prepare trainings for the relevant staff of the employees in the company;
- to improve anti-money laundering policies and procedures in the company;
- to monitor the changes and innovations in the legislation and to introduce them in the policy of the obligor in due time;

- to maintain relations with the financial regulator and law enforcement agencies;
- to ensure that the company has appropriate systems and measures for the prevention of financial crimes;
- to represent the company at forums;
- to support the introduction of changes and innovations in the strategy of the company on risk management.

In Summary of the basic requirements to counteract money laundering are:

- Identification of the client and full inspection;
- Collection and storage of the information;
- Monitoring and reporting on dubious transactions;
- Internal verification and control.

In summary, it can be said that dirty money characterizes the share and the level of informal and criminal activities and flows in all sectors of the economy and finance (which includes even the use of European funds). Therefore, they also characterize the level of formality and manageability of finance and economics. By volume and case dirty money can be judged for the informal economy and the black economics (criminal) and their impact on the official. From an economic point of view, money laundering is a major form of exchange interaction between the formal (controlled and managed) and the informal (uncontrolled and unmanageable) sector of the financial system, the tax system and the economy as a whole. It creates favorable environment and stimulates the activities of organized crime and the use of corruption. Through the use of illegal methods and huge funds, money launderers destroy the competitive environment and incentives for economic growth in the country. Conditions are created for corruption of business practices, of financial institutions, of various spheres of the economy and political governance of the state. This shows that the problem of money laundering is a risk for the whole society, because it harms its good governance, and hence the foundations. of the democratic order.

Counteraction against dirty money should be seen as a powerful mechanism for social and economic governance, the importance of which is constantly growing. It should to be considered as one of the central fields of social and economic governance and be adequately integrated into the overall system of social governance and not to be seen as a separate area in the fight against crime and to be integrated only in law enforcement.

The process of money laundering acquired by criminal activity, is dynamic and often evolves into new forms through which criminals seek to circumvent the established regulatory requirements and sanctions against their activities. Therefore, the system itself to combat and especially to combat money laundering must to be open and subject to continuous improvement

in order to it is possible to respond adequately and in time to a changing activity such as money laundering.

That is why it is important to include everyone who is vulnerable to laundry money sector of the economy in the system to counteract this crime. The active participation of those involved in money laundering is one of the main pillars of the anti-money laundering system. Within the implementation of obligations related to money laundering and cash flow channeling, and the various programs and policies proposed by international organizations fighting with this problem, good practices are formed that can serve for example to debtors from different countries who through their implementation to achieve higher efficiency in counteracting this dangerous crime for all.

2.2 OBLIGATED PERSONS

Who is obliged to report? Identification of the persons (corporate and individuals) obliged to report?

Under Art.4 of Measures against money laundering Act the persons who are obligated to report are:

1. The Bulgarian National Bank and the credit institutions, which perform activity on territory of the Republic of Bulgaria in the meaning of the Credit Institutions Act;

2. the other providers of payment services in the meaning of the Payment Services Act and the Payment Systems and their Representatives;

3. the financial institutions in the meaning of the Credit Institutions Act;

4. the currency exchange desks;

5. insurers, reinsurers and insurance firms with central offices in the Republic of Bulgaria, which have received license in the conditions and procedure of the Insurance Code, where they perform activity on or more of the insurance classes on Section I of Annex N 1 to the Insurance Code; insurers, reinsurers and insurance firms, which have received license in another Member State or other state – party of the European Economic Area Agreement (EEAA), which carry out activity on the territory of the Republic of Bulgaria, where they perform actinin on one or more classes insurances on Section I of Annex N 1 to the Insurance Code; insurers and reinsurers with central offices in states, other than a Member State, or a state – party of the EEAA, received license from the Financial Supervision Commission to carry out activity in the Republic of Bulgaria through a branch, where they carry out activity on one or more of the insurance classes under Section I of Annex N 1 to the Insurance Code;

6. leasing undertakings;

7. the post operators, licensed to carry out post money transfers under the Postal Services Act;

8. investment firms that have been licensed under the terms and procedures of the Markets in Financial Instruments Act;

9. collective investment schemes and other undertakings for collective investment that have been licensed and obtained permit under the terms and conditions of the Act on the Operation of the Collective Investment Schemes and of Other Undertakings for Collective Investment;

10. the managing companies and persons, managing alternative investment funds that have been licensed under the terms and conditions of the Act on the Operation of the Collective Investment Schemes and of Other Undertakings for Collective Investment;

11. pension security companies that have been licensed under the terms and conditions of the Code of Social Insurance with the exception of their activity on management of funds for additional compulsory pension security;

12. the registered auditors;

13. persons, who upon profession provide accounting services and/or consultations in the area of taxation;

14. persons, who upon profession provide accounting services and/or consultations in the area of taxation, as well as persons, who, as a principal business or professional activity, provide, directly or indirectly, through related persons, assistance in any form or advice on tax matters;

15. persons, who upon profession carry out legal consultations, where:

    a) they assist or participate in planning or fulfillment of an operation, transaction or other legal or factual action of their client about:

        - a purchase- sale of real estate or transfer of undertaking to a trader;
        - management of funds, financial instruments or other assets;
        - opening, managing or disposition with a bank account, with deposit account to an account for financial instruments;
        - procurement of funds for establishing a legal person or other legal formation, increasing the capital of a trade company, provision of loan or any other form of procurement of funds for realization of the activity of a legal person or other legal formation;
        - establishing, registration, organization of the activity or management of trust ownership, trader or other legal person or other legal formation;
        - trust management of property, including trusts, custodian funds and other similar foreign legal formations, established and existing pursuant to the law of jurisdictions, admitting such forms of trust ownership;

b) they act at the expense of and/or on behalf of own client in any financial operation;
c) they act at the expense of and/or on behalf of own client in any transaction with real estate;
d) they provide management address and correspondence address, office and/or other similar services for the purposed of registration and/or functioning of a legal person or other legal formation;

16. the persons who upon profession provide:

a) management address, correspondence address, office and/or other similar services for the purposes of registration and/or functioning of a legal person or other legal formation;

b) services of establishment, registration, organization of the activity and/or management of a trader or other legal person or other legal formation;

c) services of trust management of property or of a person under latter "b". including:

- fulfillment of the position or organization of execution by another person at the position of director, secretary, partner or other similar position in a legal person or other legal formation;

- execution of the position or organization of execution by another person of the position trust owner – in the cases of trusts, custodian funds and other similar foreign legal formations, established and existing according to the law of jurisdictions, admitting such forms of trusted ownership;

- execution of the position or organization of execution by another person the position of nominal shareholder in a third foreign legal person or another legal formation, other than a company, whose assets are traded on a regulated market, to which the requirements of information in compliance with the EU law or of equivalent international standards are applied;

17. the private enforcement agents and assistant private enforcement agents;

18. persons, who execute upon profession intermediation in transactions with real estates, including with respect to real estate leasing transactions, where the monthly rent amounts to, or exceeds EUR 10,000 or their equivalent in another currency;

19. wholesale traders;

20. traders of weapons, petrol and petrol products;

21. organizations of gambling games within the meaning of the Gambling Act that have obtained a license from the State Gambling Commission to organize their permitted gambling games under the procedure of Art. 3 of the same Act on the territory of the Republic of Bulgaria;

22. organizations on privatization;

23. persons, organizing awarding of public procurement;

24. ministers and municipality mayors while signing concession contracts;

25. legal persons, at which there are mutual assistance funds;

26. persons, who provide money loans against betting on items;

27. professional unions and branch organizations;

28. non-profitable legal persons;

29. professional sport clubs;

30. market operators and/or regulated markets that have been licensed under the terms and procedures of the Markets in Financial Instruments Act;

31. the central securities depositories licensed by the Financial Supervision Commission under the terms and procedures of the Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012;

32. political parties;

33. the bodies of the National Revenue Agency;

34. customs bodies;

35. the executive director of the Environment Executive Agency in his capacity of national administrator in the meaning of Commission Regulation (EU) No 389/2013 of 2 May 2013 establishing a Union Registry pursuant to Directive 2003/87/EC of the European Parliament and of the Council, Decisions No 280/2004/EC and No 406/2009/EC of the European Parliament and of the Council and repealing Commission Regulations (EU) No 920/2010 and No 1193/2011 (OJ, L 122/1 of 3 May 2013).

36. Persons, who, by occupation, trade or act as intermediaries in the trade in works of art, including when carried out by art galleries and auction houses, when the value of the transaction or related transactions amounts to, or exceeds EUR 10,000, or their equivalent in another currency;

37. Persons, who, by occupation, store, trade or act as intermediaries in the trade in works of art, when this is done in free zones and when the value of the transaction or related transactions amounts to, or exceeds EUR 10,000 or their equivalent in another currency;

38. the persons, who, by occupation provide services for the exchange between virtual currencies and recognized currencies, without gold coverage;

39. Portfolio providers, offering custody services.

In case of suspicion and/or learning about money laundering and/or about available funds with criminal origin, the persons shall be obliged to notify immediately **Financial Intelligence Directorate of the National Security State Agency,** before performing the operation or transaction, by delaying its realization in the frames of the admissible term under the normative acts, providing the relevant type of activity.

This obligation shall also occur in the cases, where the operation or transaction have not been finalized.

In the notification, the obligated persons shall indicate the maximum term, in which the operation or transaction may be suspended. In case of learning about money laundering, or about available funds with criminal origin, the obligated persons shall notify the competent bodies pursuant to the Criminal Procedure Code, the Ministry of Interior Act and the State Agency for National Security Act.

Notification of Financial Intelligence Directorate of the National Security State Agency may be made also by employees of the above persons, who are not responsible for the application of the measures against money laundering. The Directorate shall keep the anonymity of these employees.

The Financial Intelligence Directorate of the National Security State Agency shall produce to the obligated person information, related to the notification, made by him. The decision about the volume of information, which is to be produced in return for every concrete case of notification, shall be taken by the Director of the Directorate.

Information about notification about suspicion shall be exchanged in the frames of the group, unless the director of Financial Intelligence Directorate of the National Security State Agency gives other instructions.

Information about notification about suspicion shall be exchanged in the frames of the group, unless the director of Financial Intelligence Directorate of the National Security State Agency gives other instructions.

The Measure against money laundering act excludes from the circle of obliged persons, persons exercising the activity regulated by the Attorney Act only in relation to the information which these persons receive form or about some of their clients in the process of establishment of his legal situation or protection or representation of this client in or in relation to a proceeding, regulated by procedural law, which is pending, is to be formed or has finished, including in provision of legal consultation about formation or avoidance of such proceeding, notwithstanding whether this information has been received before, during or after finalization of the proceeding. This exception shall not apply, where the person exercising the activity regulated by the Attorney Act:

1. takes part in the activities on money laundering or financing terrorism;

2. provides legal advice on a request that aims to a money laundering or terrorist financing, or
3. does know, that the client seeks legal advice for the purposes of money laundering or financing terrorism.

Obligated persons according to Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015

Under Art.2 of Directive (EU) 2015/849 the obligated persons are:

1) credit institutions;
2) financial institutions;
3) the following individual or legal entity acting in the exercise of their professional activities:

a) auditors, external accountants and tax advisors;
b) notaries and other independent legal professionals, where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the:

- buying and selling of real estates or business entities;
- managing of client money, securities or other assets;
- opening or management of bank, savings or securities accounts;
- organisation of contributions necessary for the creation, operation or management of companies;
- creation, operation or management of trusts, companies, foundations, or similar structures;

Legal professionals, as defined by the Member States, should be subject to this Directive when participating in financial or corporate transactions, including when providing tax advice, where there is the greatest risk of the services of those legal professionals being misused for the purpose of laundering the proceeds of criminal activity or for the purpose of terrorist financing. There should, however, be exemptions from any obligation to report information obtained before, during or after judicial proceedings, or in the course of ascertaining the legal position of a client. Therefore, legal advice should remain subject to the obligation of professional

secrecy, except where the legal professional is taking part in money laundering or terrorist financing, the legal advice is provided for the purposes of money laundering or terrorist financing, or the legal professional knows that the client is seeking legal advice for the purposes of money laundering or terrorist financing.

c) trust or company service providers not already covered under point “a” or “b”;
d) real estate agents;
e) other persons trading in goods to the extent that payments are made or received in cash in an amount of EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
f) providers of gambling services.

Under par.2, art. 1 of Directive with the exception of casinos, and following an appropriate risk assessment, Member States may decide to exempt, in full or in part, providers of certain gambling services from national provisions transposing this Directive on the basis of the proven low risk posed by the nature and, where appropriate, the scale of operations of such services.

Among the factors considered in their risk assessments, Member States shall assess the degree of vulnerability of the applicable transactions, including with respect to the payment methods used.

Under the Directive in their risk assessments, Member States shall indicate how they have taken into account any relevant findings in the reports issued by the Commission pursuant to Article 6 of Directive.

Any decision taken by a Member State pursuant to the first subparagraph shall be notified to the Commission, together with a justification based on the specific risk assessment. The Commission shall communicate that decision to the other Member States.
Member States may decide that persons that engage in a financial activity on an occasional or very limited basis where there is little risk of money laundering or terrorist financing do not fall within the scope of this Directive, provided that all of the following criteria are met:

(a) the financial activity is limited in absolute terms;

(b) the financial activity is limited on a transaction basis;

(c) the financial activity is not the main activity of such persons;

(d) the financial activity is ancillary and directly related to the main activity of such persons;

(e) the financial activity is provided only to the customers of the main activity of such persons and is not generally offered to the public.

The first subparagraph shall not apply to persons engaged in the activity of money remittance as defined in p. 13 of Art. 4 of Directive 2007/64/EC of the European Parliament and of the Council.

For the purposes of Directive, Member States shall require that the total turnover of the financial activity does not exceed a threshold which must be sufficiently low. That threshold shall be established at national level, depending on the type of financial activity.

For the purposes of Directive, Member States shall apply a maximum threshold per customer and per single transaction, whether the transaction is carried out in a single operation or in several operations which appear to be linked. That maximum threshold shall be established at national level, depending on the type of financial activity. It shall be sufficiently low in order to ensure that the types of transactions in question are an impractical and inefficient method for money laundering or terrorist financing, and shall not exceed EUR 1 000.

For the purposes of Directive, Member States shall require that the turnover of the financial activity does not exceed 5 % of the total turnover of the individual or legal entity concerned.

In assessing the risk of money laundering or terrorist financing for the purposes of Directive, Member States shall pay particular attention to any financial activity which is considered to be particularly likely, by its nature, to be used or abused for the purposes of money laundering or terrorist financing.

- **Identification of the persons (legal entity and individuals) obliged to report**

Identification of the individuals:

Identification of clients and checkup of the identification shall be performed through using documents, data, or information from reliable and independent source. Identification of the Individuals shall be performed through production of an official identity document and making a copy of it.

With identifying individuals, data shall be collected about:

1. the names;
2. date and place of birth;
3. official personal identification number or other unique element for establishing the personality, contained in an official identity documents, whose validity term has not expired and on which there is a photo of the client;
4. every citizenship, which the person holds;
5. the state of permanent residence and address (number of post box shall not be sufficient).

With stepping in business relations, data shall be collected about the person's professional activity and the purpose and nature of the participation of the persons in the business relations by using documents data or information from a reliable independent source, filling a questionnaire, or other appropriate way.

On the basis of the risk assessment, the obligated persons may collect additional data under the conditions and procedure of the Rules on the implementation of the act.

Where the official identity document does not contain all data under Bulgarian Measures Against Money Laundering Act, collection of the missing data shall be performed by production of other official identity documents or other official personal documents, whose validity term has not expired and which contain the client's photo and a copy of them.

In case of lack of other possibility, collection of data under Bulgarian Measures Against Money Laundering Act may also be performed through production of other official documents or documents form a reliable and independent source.

Where identification is performed without the presence of the individual, subject to identification, the identification may also be performed by production of a copy of an official identity document. In these cases, the checkup of the collected identification data shall be made under Art. 55, Para. 2 of Bulgarian Measures Against Money Laundering Act.

In the cases of Art. 55, Para. 7 of under Bulgarian Measures Against Money Laundering Act, the identification of the customer and the verification of the identification data may also be carried out by means of electronic identification, the relevant certification services, provided for in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, on electronic identification and certification services in electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257/73 of 28 August 2014), hereinafter referred to as "Regulation (EU) No 910/2014", or by any other means of electronic identification or qualified certification service, recognized by a normative act, within the meaning of that Regulation, provided that the requirements of this Act and its implementing Rules, with regard to customer identification and identification verification have been fulfilled.

Identification of Legal entities

Identification of legal entities and other legal formations shall be performed by production of an original, or a notary certified copy of an official excerpt from the relevant register of their updated state and certified copy of the establishment contract, the establishment act or other document, needed for establishment of the data under Para. 4.

In the cases under Art. 23, Para. 6 of the Act on the Commercial Register and the Non-Profit Legal Entities Register and in presence of an official public trade or company register in a Member State, shall be performed by making a reference in the trade register of in the relevant public register on the file of the legal person and documentation of the undertaken actions on the identification. The conditions and procedure for documentation of the undertaken actions shall be defined by the Rules on the implementation of the act. Where the data, needed for identification of a legal person, do not fall in the scope of the circumstances, subject to entry in the trade register or in the relevant public register, are not publicly accessible or the undertaken actions are not documented, their collection shall be made under this Section and the Rules on the implementation of the act.

With identification of legal entities and other legal formations, the obligated persons under Bulgarian Measures Against Money Laundering Act shall be obliged to establish the structure of ownership, management and control of the client – legal entities or other legal formation.

With identification of legal entities and other legal formations, data shall be collected about:

1. the name;
2. the legal-organizational form;
3. the central office;
4. the management address;
5. correspondence address;
6. the updated subject of activity and the purpose or nature of the business relations or the random operation or transaction;
7. the term of existence;
8. the control bodies, the management and representation bodies;
9. type and composition of the collective management body;
10. the major place of trade activity.

Where the above documents do not contain this data, their collection shall be performed by production of other official documents.

Where a certain activity is subject to licensing, permission or registration, the clients, stepping into business relations or performing transactions or operations with or through a obligated person in relation to this activity, they shall produce a certified copy of the relevant license, permit or registration certificate.

In relation to the legal representatives of a client, - a legal entities, or another legal formation, the proxies or other individuals, who are subject to identification I relation to identification of a client – a legal entities or another legal formation, Art. 53 of Bulgarian Measures Against Money Laundering Act shall apply.

Where undertaking of measures is needed, comprising from the national risk assessment, supranational risk assessment and directions, decisions or documents, adopted by EU institutions in implementation of provision of Directive (EU) 2015/849, requirements and exceptions from this rule may be applied under conditions and procedure, defined by the Rules on the implementation of the act.

Where applicable, customer identification and verification of identification data may also be carried out by means of electronic identification, relevant certification services, provided for in Regulation (EU) No 910/2014, or by any other means of electronic identification, or qualified certification service, recognized by a normative act, within the meaning of that Regulation, provided that the requirements of this Act and its implementing Rules with regard to customer identification and identification verification, have been fulfilled.

Each Member State shall establish Financial Intelligence Units (**FIU**). The FIU have a key role in the fight against money laundering and terrorist financing. These units are responsible for receiving, requesting, analysing and disseminating information to the competent authorities on potential money laundering or terrorist financing activities. Every Member States shall notify the Commission for the name and address of their respective FIU.

A number of obliged entities and persons fall under anti-money laundering reporting requirements, such as banks, financial institutions, notaries, casinos, etc. They must file a suspicious transaction report (**STRs**) without delay to the FIU when they know or suspect that money laundering or terrorist financing is being or has been committed or attempted. On the basis of these reports, criminal investigations might be launched if necessary.

The subject to the reporting obligation is obliged to report suspicious transactions and suspected terrorism financing to the FIU. The report must be submitted regardless of whether a customer relationship has been established or has been refused, or whether the business transaction has taken place, been interrupted, or refused.

According to Directives 2015/849 and 2018/843 the obliged entities are:

1. credit institutions;
2. financial institutions;
3. the following natural or legal persons acting in the exercise of their professional activities:
   a) auditors, external accountants and tax advisors, and any other person that undertakes to provide, directly or by means of other persons to which that other person is related, material aid, assistance or advice on tax matters as principal business or professional activity;
   b) notaries and other independent legal professionals, where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the:
      i. buying and selling of real property or business entities;
      ii. managing of client money, securities or other assets;
      iii. opening or management of bank, savings or securities accounts;
      iv. organisation of contributions necessary for the creation, operation or management of companies;
      v. creation, operation or management of trusts, companies, foundations, or similar structures;
   c) trust or company service providers not already covered under point (a) or (b);
   d) estate agents including when acting as intermediaries in the letting of immovable property, but only in relation to transactions for which the monthly rent amounts to EUR 10 000 or more;
   e) other persons trading in goods to the extent that payments are made or received in cash in an amount of EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
   f) providers of gambling services;
   g) providers engaged in exchange services between virtual currencies and fiat currencies;
   h) custodian wallet providers;
   i) persons trading or acting as intermediaries in the trade of works of art, including when this is carried out by art galleries and auction houses, where the value of the transaction or a series of linked transactions amounts to EUR 10 000 or more;

j) persons storing, trading or acting as intermediaries in the trade of works of art when this is carried out by free ports, where the value of the transaction or a series of linked transactions amounts to EUR 10 000 or more.

The obliged entities are required to cooperate fully by promptly:

a) informing the FIU, including by filing a report, on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing, and by promptly responding to requests by the FIU for additional information in such cases; and
b) providing the FIU directly, at its request, with all necessary information.

All suspicious transactions, including attempted transactions, shall be reported.

In general terms and by no means exhaustive, outlined below are some examples of what might raise suspicions:

- Transactions or a series of transactions, that appear to be unnecessarily complex, making it difficult to identify the beneficial owner, or that do not appear to make economic sense;
- Transaction activities (in terms of both amount and volume) that do not appear to be in line with the expected level of activity for the customer and/or are inconsistent with the customer's previous activity;
- Transactions in excess of a customers stated income;
- Large unexplained cash lodgments;
- Loan repayments inconsistent with a customers stated income, or early repayment of a loan followed by an application for another loan of similar amount;
- Requests for third party payments. For example, this might include a third party making a payment into a customer's account to pay off a loan, to fund an investment or policy, or to fund a savings account;
- Transactions involving high-risk jurisdictions, particularly in circumstances where there is no obvious basis or rationale for doing so;
- Refusal to provide customer due diligence documentation or providing what appears to be forged documentation.

➢ **Transactions or activities to be reported**

- **Bulgaria**

According to the Bulgarian Measures Against Money Laundering Act, the obliged entities are obliged to report transactions that raise suspicion of money laundering on the basis of a set of objectives features and other circumstances like:

➢ Characteristics;
➢ Size;
➢ Nature;

- Nature of income;
- Type of business activity.

This circumstances (facts) are different for the different types of commercial or other activities and they are derived from the specifics of particular transactions and operations.

Establishing of clear criteria for identifying of the suspicious transactions or operations and clients in the activity of the obliged entities is essential for the effectiveness of anti-money laundering.

Also, the subjective element of assessing the need for reporting as a result of ongoing business/professional relationships and transactions/operations should be taken in account.

The criteria and the indicators for recognizing the suspicious transactions/operations and clients are a non-exhaustive list of anomalies related to the objective form of each different category of transactions.

In most cases, the objective content of the transaction is neutral in itself and therefore does not allow the true purpose to be established immediately. Deals that are common in terms of amounts, deliverables, distribution channels, and geographic location for clients with certain characteristics could prove disproportionately large or economically unjustified for other clients.

Therefore, in the in the event that one or more criteria are established, persons implementing anti-money laundering measures should carry out a further examination of all available information as well, to collect additional information in order to be able to assess the nature of the transaction/operation, individual actions/circumstances and to distinguish between those who raise doubts.

In case of suspicion and/or learning about money laundering and/or about available funds with criminal origin, the obliged entities must notify immediately FIU before performing the operation or transaction, by delaying its realization in the frames of the admissible term under the normative acts, providing the relevant type of activity.

When the delay of the operation or transaction is objectively impossible or there is possibility this to hinder the prosecution actions of the beneficiaries of the suspicious transaction or operation, the obliged entities must notify the FIU immediately after its realization, by indicating the reasons because of which the delay has been impossible. The obligation for notification also occur in the cases when the operation or transaction have not been finalized.

In addition, it should be noted that the submission of a report on suspicious transactions should be made immediately after the suspicion has been raised or identified.

The obliged entities must keep a special diary for:

- All notifications from staff members for a suspected money laundering or for the presence of funds with criminal origin, together with a conclusion about the need to notify FIU;

- A conclusion for the purpose and nature of complex or unusually large transactions/operations, in transactions or operations, performed under unusual schemes, as well as in operations and transactions without explicit economic or legal purpose, as well as conclusions regarding suspicions of money laundering or presence of funds with criminal origin.

The obliged entities shall notify the FIU about every payment in cash in the value of BGN 30 000 or their equivalence in a foreign currency, made by, or to their client in the frames of the established relations or in random transactions or operations. This information is provided on a monthly basis until the 15th of the month following the month to which the information relates.

- **Malta**

As a European Union member state, Malta has implemented all EU Directives regulating the prevention of money laundering. Furthermore, Malta is part of MONEYVAL (the Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures formerly PC-R-EV), established in September 1997 by the Committee of Ministers of the Council of Europe to conduct self and mutual assessment exercises of the anti-money laundering measures implemented in Council of Europe countries.

Whenever obliged entities know, suspect or have reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to financing of terrorism, or that a person (natural or legal) may have been, is or may be connected with money laundering or financing of terrorism they are required to disclose that information to the Financial Intelligence Analysis Unit (**FIAU**).

- **Germany**

The obliged entities in Germany must comply with the obligation to submit suspicious transaction reports. Such matters must be reported, irrespective of the value of the wealth in question or the amount of the transaction involved, to the German Financial Intelligence unit without delay.

According to Section 43 from the German Money Laundering act (Geldwäschegesetz – **GwG**), the obliged persons report when fact indicate that:

a) property related to a business relationship, brokerage or transaction is derived from a criminal offence which could constitute a predicate offence for money laundering;
b) a business transaction, a transaction or property is related to terrorist financing; or
c) the contracting party has not fulfilled its obligation under section 11 (6), sentence 3 of the GwG to disclose to the obliged entity whether it intends to establish, continue or conduct the business relationship or transaction on behalf of a beneficial owner.

The obliged entity should report this matter, irrespective of the value of the property in question or the amount of the transaction involved.

The suspicious transaction reporting obligation is tied to the previously known preconditions.

- **Austria**

The obliged entities shall inform the Austrian Financial Intelligence Unit (Geldwäschemeldestelle) without delay upon their own initiative by means of a suspicious activity report, if they know, suspect or have reasonable grounds to suspect, that:

a) an attempted, upcoming, ongoing or previously conducted transaction is related to asset components originating from criminal activities (including asset components which stem directly from a criminal act on the part of the perpetrator);
b) an asset component originates from criminal activities listed (including asset components which stem directly from a criminal act on the part of the perpetrator);
c) a customer has violated the obligation to disclose trust relationships pursuant;
d) the attempted, upcoming, ongoing or previously conducted transaction or the assets are connected to a criminal organisation pursuant, a terrorist organisation, a terrorist crime pursuant or terrorist financing pursuant.

The reporting obligations of the obliged entities exist with regard to suspicious activities. When an obliged entity has reason for suspicion that a transaction/operation or activity is relates to proceeds from predicate offence, the obliged entity must report.

- **Romania**

According to Law no. 129/2019 to prevent and combat money laundering and terrorism financing, as well as to amend and supplement some legislative act (**Law 129**) the obliged entities are required to report suspect transactions exclusively to the Romania FIU if they know, suspect or have reasonable grounds to suspect that:

a) the goods come from offenses or are related to terrorism financing;
b) the person or proxy/representative/trustee is not who he/she claims to be;
c) the information that the reporting entity holds may be used to enforce the provisions of this law;
d) in any other circumstances, or with respect to the elements of such a nature as to raise a lot of questions about the nature, purpose, or motivation of the transaction, such as the existence of certain anomalies in comparison with the profile of the customer, as well as when there is an indication that the data possessed about a customer or the real beneficiary are not real, or out of date, and the client is refusing to update or provide explanations that are not plausible.

The obliged entities submit a report for suspect transaction to the FIU when the objective factual circumstances related to a business relationship or occasional transaction correspond in whole or in part to the indicators or typologies of suspect transactions publicly presented by the Romanian FIU.

The obliged persons shall immediately forward to the FIU the report on suspect transactions prior to any transaction related to the customer connected with the reported suspicion.

- **Belgium**

The obliged entities have to report a suspicion to Belgium FIU when they know, suspect or have reasonable grounds to suspect:

a) that funds, regardless of the amount, are related to money laundering or terrorist financing;
b) that transactions or attempted transactions are related to money laundering or terrorist financing. This obligation also applies when the customer decides not to carry out the intended transaction;
c) a fact of which they are aware are linked to money laundering.

The obliged entities have to report suspicious fund, transactions or attempted transactions and facts, of which they know are part of activities carried out by them in another Member State without having a subsidiary, branch or other type of establishment through agent or distributors representing them there.

Also, the Belgium Anti-Money Laundering Law empowers the King to determine, by Royal Decree deliberated in the Council of Ministers and adopted upon the advice of FIU, situations in which funds, transactions and facts should in any case be reported.

- **Croatia**

According to the Croatian Anti-Money Laundering and Terrorism Financing Law the obliged entities are obliged to refrain from carrying out a suspicious transaction when they know, suspect or have reason to suspect that there are reasons for suspicion of money laundering or terrorism financing in relation to the suspicious transaction.

The obliged entities are obliged to inform the Croatian FIU without any delay and prior to carrying out the suspicious transaction as well as to state in the report the deadline within which the transaction will be performed.

According to the Croatian Anti-Money Laundering and Terrorism Financing Law as a suspicious transaction is considered each attempted or performed cash and non-cash transaction, regardless of its value and the manner of performing it, when:

a) the obliged entities know, suspect or have reasons to suspect that the transaction includes funds derived from a criminal activity or is linked with terrorist financing;
b) indicators for recognizing suspicious transactions, funds and persons indicate that there are reasons for the suspicion of money laundering or terrorist financing;
c) the transaction corresponds to the typologies or trends of money laundering or terrorist financing;
d) when obliged entities estimate that in relation to the transaction, funds or customer there are also other reasons for the suspicion of money laundering or terrorist financing.

If the obliged entities know, suspect or have reasons to suspect that the funds, regardless of their amount, represent proceeds of a criminal activity or are related to terrorist financing, they shall be obliged to inform the Croatian FIU of that without any delay.

Also, lawyers, law offices, public notaries, audit companies, independent auditors, external accountants that are legal or natural persons carrying out accounting services, tax advisers and tax advisory companies, when carrying out their activities, shall be obliged to inform the Croatian FIU for suspicious transactions, fund and persons. This entities shall be obliged every time a customer asks for them for advice in relation to money laundering or terrorist financing to inform the FIU of that not later than the following working day.

- **Greece**

According to Law 4557/2018, the obliged persons are required to:

a) promptly informing the FIU, on their own initiative, where they know, suspect or have reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing. All suspicious transactions, including attempted transactions, shall be reported;
b) promptly providing the FIU, the competent authority and other public authorities entrusted with duties for suppressing money laundering and terrorist financing, at their request, with all necessary information, in accordance with the procedures under the provisions in force.

- **Hungary**

According to Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (**Act LIII**) the obliged entities shall report to FIU without delay any information, fact or circumstance giving rise to a suspicion:

a) of money laundering;
b) of terrorist financing; or
c) that specific property is derived from criminal activity.

- **Ireland**

The requirement to report suspicious transactions for the obliged entities in Ireland is contained in section 42 of the Criminal Justice (Money Laundering and Terrorist Financing) Act, 2010 (**CJA 2010**). According to the provisions of CJA 2010 the obliged entities which knows, suspects or has reasonable grounds to suspect, on the basis of information obtained in the course of carrying on business their business activities, that another person has been or is engaged in an offence of money laundering or terrorist financing shall report to Ireland FIU and the Revenue Commissioners.

The obliged entities shall make the report as soon as practicable. As soon as practicable is when the obliged entity suspects or has reasonable grounds to suspect money laundering or terrorist financing before the execution of a transaction or at the same time as the execution of a transaction. In such cases, the obliged entity should immediately file a suspicious transaction report. The obliged entity may need to conduct further analysis and investigation in order to make its determination. Any such analysis and investigation should be conducted without delay.

- **Lithuania**

According to the Law of the Republic of Lithuania on Prevention of Money Laundering and Terrorist Financing, the obliged entities must immediately, not later than within one working day from the emergence of such knowledge or suspicions, report to the FIU if they know or suspect that property of any value is, directly or indirectly, derived from a criminal act or from involvement in such an act, also if they know or suspect that such property is used to support one or several terrorists or a terrorist organisation.

The obliged entities must pay attention to any activities which they regard as likely, by its nature, to be related to money laundering and/or terrorism financing and in particular are:

- too complex or unusually large transactions;
- have unusual patterns;
- transactions which have no apparent economic or visible lawful purpose,;
- business relationships or monetary operations with customers from third countries in which, based on the information officially published by international intergovernmental organisations, money laundering and/or terrorism financing prevention measures are insufficient or do not correspond to international standards.

- **Poland**

With the new Act of 1 March 2018 on Counteracting Money Laundering and Financing of Terrorism (**ACMLFT**) the Poland legislation creates a lot of reporting obligations about their obliged entities. The general principle is that the obliged entities shall notify the FIU for any circumstances which may indicate the suspicion of committing the crime of money laundering or financing of terrorism.

The obligated entities shall immediately notify FIU, with the use of electronic communication means, of any case of acquiring justified suspicion that the specific transaction or specific assets may be associated with money laundering or financing of terrorism.

We will take a closer look at the reporting obligations of the Polish obliged entities in the section below.

- **Portugal**

According to the Portugal Law No. 83/2017, of August 18, the obliged entities, on their own initiative, shall immediately report to the Central Department of Investigation and Criminal Action of the Attorney General's Office and the FIU whenever they know, suspect or have sufficient reasons to suspect that certain fund or other assets, regardless of the amount or value involved, come from criminal activities or are related to money laundering or terrorism financing.

- **Spain**

According to Law 10/2010 of 28 April, on the prevention of money laundering and terrorist financing, the obliged entities shall pay special attention to any event or transaction, regardless

of its size, which, by its nature, could be related to money laundering or terrorist financing. In particular, obliged entities shall examine with special attention all complex or unusual transactions or patterns of behavior's or those with no apparent economic or visible lawful purpose, or which denotes signs of deception or fraud.

The obliged entities shall, on their own initiative, notify without delay FIU of any act or transaction, even the mere attempt, regarding which there is any indication or certainty that it bears a relation to money laundering or terrorist financing.

The FIU shall be notified of transactions that reveal an obvious inconsistency with the nature, volume of activity or customer operating history, provided that does not perceive any economic, professional or business justification for the execution of the transactions.

- **Sweden**

The money laundering and terrorism financing in Sweden is regulated by Law (2017: 630) on measures against money laundering and terrorist financing. According to this Law, if the obliged entity has reasonable grounds to suspect money laundering or terrorism financing or that property is otherwise the result of a criminal act, information on all circumstances that may indicate this should be reported to the FIU without delay.

Proof of money laundering or terrorist financing does not need to exist. Even the slightest suspicion is enough for the obliged entities to be obliged to report.

All obliged entities (according to the Swedish Anti-Money Laundering Act) conducting business in Sweden, have an obligation to file an annual report to the Swedish FIU. Foreign entities conducting business in Sweden only have an obligation to send an annual report in respect of the business that have been conducted in Sweden. This means that if a branch of a foreign company has been set up and operates in Sweden, the branch only has an obligation to report in respect of the Swedish branch, not of the foreign company. The obliged entities are required to make this report no later than 31 March each year.

Reporting thresholds:

- **Bulgaria**

The obliged entities shall notify the FIU about every payment in cash in the value of BGN 30 000 or their equivalence in a foreign currency, made by, or to their client in the frames of the established relations or in random transactions or operations. This information is provided on a monthly basis until the 15th of the month following the month to which the information relates.

- **Germany**

The reporting obligations of the obliged entities are not bound by specific thresholds. The German obligations refers only to circumstances which appear suspicious. The value of the transaction/operation is not explicitly stated as a triggering factor of the reporting obligation.

- **Austria**

The reporting obligations of the obliged entities are not bound by specific thresholds.

- **Romania**

The obliged entities in Romania have the obligation to report to the FIU cash transactions, in lei or foreign currency, whose minimum limit represents the equivalent in lei of 10 000 euro.

The credit and financial institutions in Romania, shall submit on-line reports regarding the external transfers in and from accounts, in lei or in foreign currency, whose minimum limit represents the equivalent in lei of 15 000 euro.

Also, a reporting obligation is provided in case of money remittance operations with funds exceeding the RON equivalent of EUR 2,000.

- **Belgium**

The reporting obligations of the obliged entities are not bound by specific thresholds.

- **Croatia**

According to the Croatian Anti-Money Laundering and Terrorism Financing Law the obliged entities are obliged to inform the FIU of the transaction that is carried out in cash in the amount of HRK 200 000 and more, not later than within three days from the day of performance of the transaction.

- **Greece**

The reporting obligations of the obliged entities are not bound by specific thresholds.

- **Hungary**

The reporting obligations of the obliged entities are not bound by specific thresholds.

- **Ireland**

There is no minimum monetary threshold for reporting and no amount should be considered too low for suspicion

- **Lithuania**

The reporting obligations of the obliged entities are not bound by specific thresholds.

- **Poland**

According with article 72 from ACMLFT, the Polish obliged entities, with some exceptions, shall provide the FIU with information on:

- accepted payments or executed disbursement of fund exceeding the equivalent of EUR 15 000;
- executed transfer of fund exceeding the equivalent of EUR 15 000, excluding:
    a) transfer of funds between the payment account and the term deposit account held by the same customer with the same obligated entities;
    b) domestic transfer of funds from other obligated entities;
    c) transaction associated with own management of the obligated entities which was executed by the obligated entities in its own name and on its own behalf, including a transaction concluded on the interbank market;
    d) transaction executed for and on behalf of public finance sector entities;
    e) transaction performed by a bank associating cooperative banks, if the information on the transaction was provided by an associated cooperative bank;
    f) transaction of temporary lien to secure assets, performed for the duration of the lien agreement with the obligated entities.

The obligated entities shall provide the FIU with information concerning the executed purchase and sale transaction of foreign currency with the value exceeding the equivalent of EUR 15000, or intermediation in performing such transaction.

- **Portugal**

The reporting obligations of the obliged entities are not bound by specific thresholds. All suspicious transactions shall be reported, regardless of the amounts involved.

- **Spain**

The reporting obligations of the obliged entities are not bound by specific thresholds. However, certain categories of the obliged entities must report on a monthly basis (systematic reporting) to FIU.

- **Sweden**

The reporting obligations of the obliged entities are not bound by specific thresholds.

Regulator / authority in Bulgaria, Malta, the Netherlands

- **FIU of Bulgaria**

The National Security State Agency of Bulgaria created a specialized administrative directorate "Financial Intelligence" which receives, stores, investigates, analyzes and discloses financial intelligence information under the terms and procedures of the Measures against Money Laundering Act (**MAMLA**) and the Measures against financing of terrorism Act (**MAFTA**).

The Directorate is a financial intelligence structure of the Republic of Bulgaria within the meaning of Art. 2, § 1 and 3 of Council Decision dated 17 October 2000. The directorate "Financial Intelligence" have the following functions:

- prevention;
- detection and counteraction of money laundering and terrorist financing, including in connection with capital movements,
- detection and counteraction of corruption;
- detection and counteraction of bribery in international commercial transactions and confiscation.

The Directorate may receive information about money laundering from a state bodies, apart through the obliged entities. The supervision bodies shall be obliged to provide information to Directorate immediately if doing their supervision activity, they find facts which may be related to money laundering.

Also, the Directorate may receive information about suspicion for money laundering through international exchange, except through the obliged entities. The Directorate upon own initiative and upon request, shall exchange information about suspicion for money laundering also for related predicate crimes with the relevant international bodies, EU bodies and bodies of other states on the basis of international agreements and/or under mutual conditions.

The National Security Agency, through the Financial Intelligence Directorate, works closely with the Financial Action Task Force (FATF), an organization that sets standards against money laundering and terrorist financing, and with MONEYVAL (Committee of Experts on Evaluation Council of Europe Anti-Money Laundering Organization), an organization responsible for Europe for the prevention of money laundering.

- **FIU of Malta**

The Financial Intelligence Analysis Unit (**FIAU**) is a national Maltese institution responsible for preventing money laundering and financing terrorism. The Financial Intelligence Analysis Unit is responsible for collecting and investigating financial crime information. Malta established this institution with "Prevention of Money Laundering Act" (**PMLA**).

While the FIAU is the national agency with the responsibility for prevention of money laundering and financing of terrorism and has the function to supervise compliance by all obliged entities, including financial services operators with the anti-money laundering and combating financing of terrorism legislative provisions, the Malta Financial Services Authority (**MFSA**), as the financial services supervisory authority has a vested regulatory interest to prevent the use and involvement of authorized persons in such crimes.

The MFSA as supervisory authority is considered to be an agent of the FIAU and is required to extend assistance and cooperation to the FIAU in the fulfilment of its responsibilities under the PMLA. Accordingly, the FIAU may request the MFSA to provide it with information of

which it may become aware during the course of its supervisory functions, including that a obliged entity may not be in compliance with the requirements of the PMLA.

The MFSA and FIAU conduct jointly supervision on money laundering and financing of terrorism. They main purpose is to monitor compliance by financial services license holders with the applicable AML/CFT laws, regulations and the Implementing Procedures issued by the FIAU, and where necessary to take appropriate action, including remedial, enforcement and sanctioning measures.

The obliged entities in Malta must meet Customer Due Diligence requirements and report suspicious transactions to authorized units.

- **FIU of Germany**

The Central Office for Financial Transaction Inquiries is the national central office for receiving, collecting and evaluating reports of suspicious financial transactions that may be related to money laundering or terrorist financing.

- **FIU of Austria**

The Money Laundering Reporting Office takes reports from professional groups subject to the reporting obligation regarding suspicious transactions in accordance with the Financial Market Money Laundering Act, the Accounting Bookkeeping Act, the Stock Exchange Act, the Commercial Code, the Gambling Act, the Corporate Tax Act, the Notaries and Lawyers Act, the Chartered Accountants Act and the Customs Law Implementation Act.

- **FIU of Romania**

The FIU of Romania is the National Office for Prevention and Control of Money Laundering (**NOPCML**). NOPCML have a leadership role on drafting, coordinating and implementation of the national system for combating money laundering and terrorism financing. NOPCML started its activity in 1999, functioning as specialized body with legal personality, subordinated to the Government of Romania. The main functions include:

- receiving, analyzing and processing financial information;
- supervision, verification and control of the reporting entities which are not, according to the law, under the prudential supervision of other authority;
- prevention and combating terrorism financing acts;
- prevention and combating terrorism financing acts;
- cooperation with national and international authorities

- **FIU of Belgium**

The Belgium FIU is named Financial Intelligence Processing Unit (**FIPU**) and is established, responsible for processing and disseminating information with a view to combating money

laundering and financing of terrorism, as well as the financing of the proliferation of weapons of mass destruction.

The FIPU is operationally independent and autonomous, which means that it has the authority and capacity to carry out its functions freely, including the ability to take autonomous decisions to analyse, request and disseminate specific information it receives. It is under the administrative supervision of the Minister of Justice and the Minister of Finance.

- **FIU of Croatia**

The FIU of Croatia is the Anti-Money Laundering Office (**CAMLO**). The CAMLO is the central national body in charge for receiving, analysing and disseminating to competent bodies cases with suspicion of money laundering and financing terrorism, is a part of the preventive system and an intermediary body, between financial and non-financial sector

CAMLO is established according to Croatian Anti-Money Laundering and Terrorism Financing Law, as special and operational independent unit within Ministry of Finance.

- **FIU of Greece**

The FIU of Greece is named Anti-Money Laundering Authority. The Authority's purpose is the collection, the investigation and the analysis of suspicious transactions reports that are forwarded to it by legal entities and natural persons, under special obligation, as well as every other information that is related to the crimes of money laundering and terrorist financing, proliferation of weapons of mass destruction financing, and the source of funds investigation.

The Authority is administratively and operationally independent. Its headquarters are in the Prefecture of Attica, at a place designated by decision of the Minister of Finance, upon proposal of its President. The budget of the Authority is part of the budget of the Ministry of Finance.

- **FIU of Hungary**

The FIU of Hungary is named Hungarian Financial Intelligence Unit (**HFIU**). HFIU is in charge of receiving, analysing, disseminating suspicious transaction/activity reports and shall perform analysis and assessment with a view to combating money laundering and terrorist financing, and for the purpose of prevention, detection and investigation of criminal activities, including operational and strategic analyses.

- **FIU of Ireland**

The FIU of Ireland is part of the Garda National Economic Crime Bureau and is a national reception point for Suspicious Transaction Reports submitted under Irish Money Laundering legislation by all the obliged entities. The FIU is supported by the Money Laundering Investigation Unit (MLIU).

The functions of FIU includes:

- Receipt, analysis and dissemination for investigation of STRs to relevant Garda units;
- the FIU analyses and disseminates STRs and intelligence gained, to other national units within An Garda Síochána and Gardaí throughout the country for investigation and potential further action;
- the obliged entities are required to report STRs to both the FIU and the Office of the Revenue Commissioners;
- the FIU analyses STRs which have potential domestic or international terrorist financing links;
- the FIU actively cooperates with law enforcement agencies in other jurisdictions in matters relating to suspected money laundering and terrorist financing;
- the FIU provides training to members of An Garda Síochána throughout the country to create awareness of the value of financial intelligence in the fight against money laundering, terrorist financing and all criminality.

- **FIU of Lithuania**

The Lithuanian FIU is the Financial Crime Investigation Service (**FCIS**) and its responsible for the implementation of money laundering and terrorism financing prevention measures. The activity of FCIS is aimed at creating an effective national anti-money laundering system and to ensures its proper functioning.

- **FIU of Poland**

The FIU of Poland is form by the General Inspector of Financial Information (**GIFI**) and the Department of Financial Information which supports the GIFI activities. The GIFI task is to prevent a potential crimes of money laundering and financing terrorism. The GIFI obtains, gathers, processes and analyses information which can be connected e.g. with money laundering or financing terrorism.

- **FIU of Portugal**

The obliged entities in Portugal shall report to the Portugal's FIU and the Central Department of Investigation and Criminal Action. Portugal's FIU operates independently as a department of the Portuguese Judicial Police. At the national level, the FIU is responsible for gathering, centralizing, processing, and publishing information pertaining to investigations of money laundering and tax crimes. It also facilitates cooperation and coordination with other judicial and supervising authorities. At the international level, the FIU coordinates with the other countries FIUs.

- **FIU of Spain**

The Spanish FIU is the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences (**SEPBLAC**). SEPLAC is also the Supervisory Authority in relation to the prevention of money laundering and terrorist financing. SEPLAC analyses several information sources and in those cases in which signs or certainty of money laundering or terrorist financing are detected, produces financial intelligence reports. SEPLAC performs

strategic analysis functions to identify patterns, trends and typologies on money laundering or terrorist financing.

- **FIU of Sweden**

The Swedish FIU (**FIPO**) is established as a branch of law enforcement, within the Police Authority. FIPO is oversees all intelligence work regarding anti-money laundering and financing of terrorism. The obliged entities must report to FIPO suspicious transaction reports on money laundering and terrorism financing.

2.3. RISK COUNTRIES AND GEOGRAPHICAL ZONES

Pursuant to Article 9 (1) of Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, in order to protect the proper functioning of the internal market, third countries whose strategic weaknesses in their national anti-money laundering and anti-terrorist financing rules pose a significant threat to the Union's financial system are known as **high-risk third countries**.

Article 9 (2) of this Directive empowers the Commission to adopt delegated acts in order to identify high-risk third countries, taking into account their strategic weaknesses, and sets out the criteria on which the Commission's assessment should be based. On the basis of this identification, obligated entities should apply measures for extended comprehensive customer due diligence when establishing business relationships or transactions with individuals or legal entities established in the listed countries, in accordance with Article 18 (1) of the Fourth anti-money laundering directive.

Because of the obligation that the European Commission has – to identify the countries that have strategic weaknesses in their national anti-money laundering and anti-terrorism financing rules, On 7 May 2020 was issued on a Commission Delegated Regulation 2020/855 amending Delegated Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council. This is the latest Regulation which determines the high-risk third countries for 2020.

Factors that identify a country as a 'high risk' country

1. **Geographical location;**
2. **Presence of strategic weaknesses in the national framework;**

Strategic weaknesses are determined on the basis of the following criteria:

1. the legal and institutional framework of the country concerned in relation to four key requirements:

a) criminalizing money laundering and terrorist financing;
b) comprehensive customer inspection;
c) information storage;
d) reported suspicious transactions;

2. the powers and procedures of the competent authorities of the third country for the objectives of the fight against money laundering and terrorist financing;
3. the effectiveness of the anti - money laundering and anti - money laundering system terrorism to address the risks of these activities in the third country.

Among the key criteria, the assessment of the effectiveness of measures to combat money laundering and the financing of terrorism. The aim is to assess not only whether the legal framework is in line with requirements on combating money laundering and terrorist financing, but and whether these measures are applied effectively. The Commission refers to already established indicators and reports on a number of jurisdictions prepared and published by specialized global authorities, such as the reports of the Financial Action Task Force (FATF).

Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) is an intergovernmental organization, which:

1. sets standards and assists the effective implementation of the anti-money laundering measures on international level;

2. aims to help for the fight against money laundering, terrorist financing and other related threats to the integrity of the international financial system.

The FATF has developed **Recommendations,** knowns as FATF Recommendations or FATF Standards, which ensure a co - ordinated global response to prevent organized crime, corruption and terrorism. They help authorities go after the money of criminals dealing in illegal drugs, human trafficking and other crimes. Another main purpose for FATF is to be stopped funding for weapons of mass destruction.

The FATF is working on money laundering and terrorist financing techniques and continuously strengthens its standards to address new risks, such as the regulation of virtual assets, which have spread as cryptocurrencies gain popularity. The FATF monitors countries to ensure they implement the FATF Standards fully and effectively, and holds countries to account that do not comply.

The FATF identifies jurisdictions with weak measures to combat money laundering and terrorist financing (AML/CFT) in two FATF public documents that are issued three times a year.

1)The first public document, the statement **"High-Risk Jurisdictions subject to a Call for Action"** (previously called "Public Statement"), identifies countries or jurisdictions with serious strategic deficiencies to counter money laundering, terrorist financing, and financing of proliferation. For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence, and in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the ongoing money laundering, terrorist financing, and proliferation financing risks emanating from the country. This list is often externally referred to as the “black list”.

2) The statement **"Jurisdictions under Increased Monitoring"** (previously called “Improving Global AML/CFT Compliance: On-going process”) identifies countries that are

actively working with the FATF to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing. When the FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring. This list is often externally referred to as the 'grey list'.

"High risk third country" - Countries that do not apply or apply incomplete international standards in combating money laundering, defined by the European Commission by Delegated Regulation (EU) 2016/1675 of Commission of 14 July 2016 supplementing Directive (EU) 2015/849 of European Parliament and the Council by identifying high-risk third parties countries with strategic weaknesses.

List of high-risk countries under regulations of the EU and Lists of the FATF:

High risk third country under Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016

1. Afghanistan
2. The Bahamas
3. Barbados
4. Botswana
5. Cambodia
6. Ghana
7. Iraq
8. Jamaica
9. Mauritius
10. Mongolia
11. Myanmar/ Burma
12. Nicaragua

13. Pakistan

14. Panama

15. Syria

16. Trinidad and Tobago

17. Uganda

18. Vanuatu

19. Yemen

20. Zimbabwe

High risk third country under Commission Delegated Regulation (EU) 2020/855 of 7 May 2020

1.Afghanistan

2.The Bahamas

This is a list of third countries whose strategic weaknesses in their national anti-money laundering and anti-terrorist financing framework pose a significant threat to the Union's financial system.

In accordance with Article 18 of Directive (EU) 2015/849, obligated entities from all Member States must apply measures for extended comprehensive customer due diligence in their relations with natural persons or legal entities established in high-risk third countries.

2.4 TERRORISM FINANCING

Concepts:

- **Terrorism** is any act of a criminal nature accompanied by an act of violence, which by endangering the safety and lives of citizens, as well as important infrastructure sites, aims to create fear and insecurity in society and to destabilize institutions as a means to achieve specific political and ideological goals. Terrorism is a global threat and is not linked to a specific religion, ideology, ethnicity or civilization.

- **Violent extremism** is a phenomenon in which individuals or groups support or commit ideologically motivated violence in order to achieve their ideological goals.

- **Radicalization** is a process during which the extreme of opinions, views, beliefs and ideologies to the point of fierce rejection of alternative to the ideas preached. Radicalization is characterized by decisive willingness to impose their own views and principles over those of the rest of society by rejecting the constitutional foundations of democracy and non-recognition of fundamental human rights

What is terrorism financing?:

- The financing of a terrorist activity is the search for, receipt or provision of funds with the intention of using them in support of terrorist acts or organizations. These funds can come from both legal and illegal sources.
- According to the International Convention for the Suppression of the Financing of Terrorism, a person commits an offense called "terrorist financing" in the following circumstances: "when that person provides or receives funds, directly or indirectly, lawfully or unlawfully, with the knowledge that they will be used in whole or in part to commit an offense which falls within the scope of the Convention.
- The persons or groups that deal with the financing of terrorist activity do not necessarily conceal a source of money, but conceal both the financing and the nature of the financed activity.

What are counter – terrorism financing (ITF) measures?:

The term ‘counter-terrorism financing measures’ refers specifically to all policies and legislation that force financial institutions to proactively monitor their customers in order to prevent terrorist financing activities.

Example for ‘counter-terrorism financing measures’ is the ***UN Global Counter-Terrorism Strategy.***

- **The UN Global Counter-Terrorism Strategy** (A/RES/60/288) is a unique global instrument to enhance national, regional and international efforts to counter terrorism. Through its adoption by consensus in 2006, all UN Member States agreed the first time to a common strategic and operational approach to fighting terrorism.

The Strategy does not only send a clear message that terrorism is unacceptable in all its forms and manifestations but it also resolves to take practical steps, individually and collectively, to prevent and combat terrorism. Those practical steps include a wide array of measures ranging from strengthening state capacity to counter terrorist threats to better coordinating UN System’s counter-terrorism activities.

- **Pillars of the UN Global Counter Terrorism Strategy**

The UN Global Counter-Terrorism Strategy in the form of a resolution and an annexed Plan of Action (A/RES/60/288) is composed of 4 pillars, namely:

- Addressing the conditions conducive to the spread of terrorism;
- Measures to prevent and combat terrorism;
- Measures to build states' capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in that regard;
- Measures to ensure respect for human rights for all and the rule of law as the fundamental basis for the fight against terrorism.

The UN General Assembly reviews the UN Global Counter-Terrorism Strategy every two years, making it a living document attuned to Member States' counter-terrorism priorities.

Another example is ***Consolidated list of persons, groups and entities subject to EU financial sanctions.***

The correct application of financial sanctions is crucial in order to meet the objectives of the Common Foreign and Security Policy and especially to help prevent the financing of terrorism. The application of financial sanctions constitutes an obligation for both the public and private sector. In this regard, the EU assigns particular responsibility to credit and financial institutions, since they are involved in the bulk of financial transfers and transactions affected by the relevant Regulations.

There is another list that includes all individuals and entities subject to measures imposed by the Security Council. That is the **United Nations Security Council Consolidated List.**

The inclusion of all names on one Consolidated List is to facilitate the implementation of the measures, and neither implies that all names are listed under one regime, nor that the criteria for listing specific names are the same. For each instance where the Security Council has decided to impose measures in response to a threat, a Security Council Committee manages the sanctions regime. Each sanctions committee established by the United Nations Security Council therefore publishes the names of individuals and entities listed in relation to that committee as well as information concerning the specific measures that apply to each listed name.

Member States are obliged to implement the measures specific to each listed name as specified on the websites of the related sanctions committee.

Countering terrorism

There are four main areas of activity:

- **Prevention** - by identifying and taking specific measures regarding the factors contributing to the radicalization of individuals and groups, as well as to prevent their becoming terrorists. The activity of prevention against involvement in terrorist activity is systematically related to the activity of prevention of radicalization.
- **Protection** of citizens and sites from the critical infrastructure of the state. Reducing the potential vulnerability of society in the event of a terrorist attack is essential.
- **Counteracting** direct terrorist activity, which is real

threat, through the collection of intelligence, investigation of received signals and threats, dismantling of terrorist and extremist groups, destruction of the channels for financing terrorist activities, as well as prevention of persons involved in terrorist activities to acquire weapons of mass destruction. Bringing charges and bringing terrorists to justice.

- **Overcoming the consequences** of direct terrorist activity through an adequate response of the competent structures.

2.5 BENEFICIAL OWNERSHIP

Beneficial ownership is a term in domestic and international commercial law which refers to the natural person or persons 'who ultimately own or control a legal entity or arrangement, such as a company, a trust, or a foundation'.

Ultimate Beneficial Owner refers to the natural persons 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 entities or arrangement. Reference to 'ultimately owns or controls' and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control. This definition should also apply to beneficial owner or a beneficiary under a life or other investment-linked insurance policy (FATF guidelines).

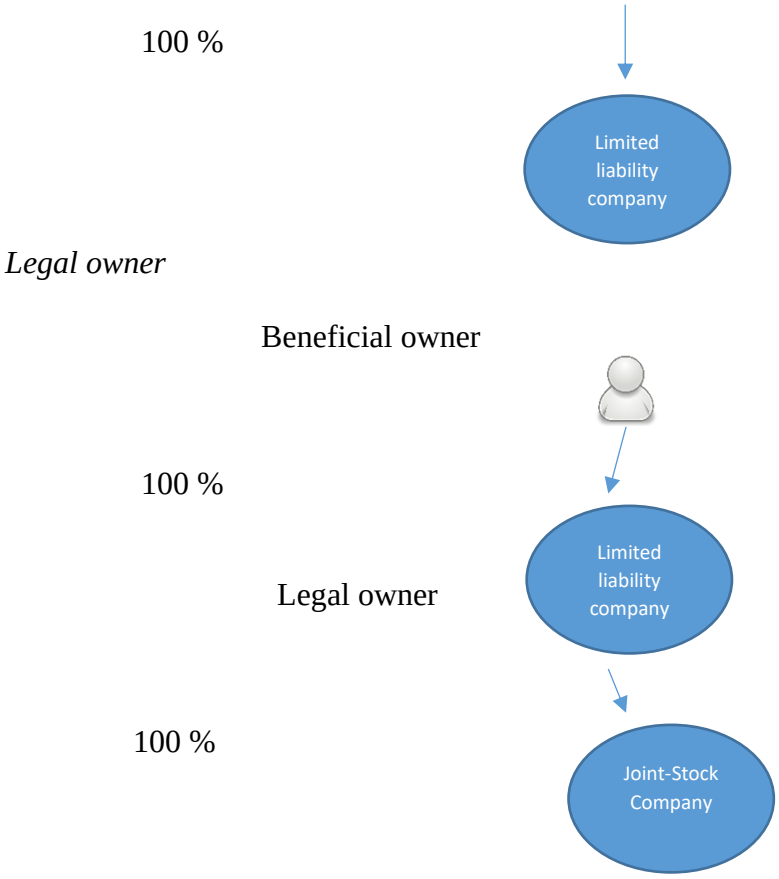
Control may be evident in influence over or a veto of the decisions that an entity makes, through agreements among shareholders or members, through family links or other types of connections with decision makers, or by holding negotiable shares or convertible stock from an entity.

It's important to identify the Beneficial Owner because his anonymity enables many illegal activities to take place hidden from law enforcement authorities, such as tax evasion, corruption, money laundering, and financing of terrorism.

When an individual is the sole shareholder of a company and controls it directly, that individual is the beneficial owner of the company. However, there may be more layers involved in the ownership structure, perhaps a chain of entities.

Figure *Difference between a Beneficial Owner and a Legal Owner*

Beneficial owner



The longer the chain of entities is and the more jurisdictions the entities span, the harder it is to identify the Beneficial Owner, given the need to determine who controls each of the layers.

Another factor that makes it difficult to identify the Beneficial Owner is the nominees. The use of nominees, whereby an entity allows its name to appear as a shareholder or owner in the name of someone else (whose identity remains hidden) is prohibited in some countries but legal in others. This way the nominee shareholders mask/hides the real Beneficial Owner in the top of the companies chain.

Bearer shares and bearer share warrants can also be used to hide the identity of the company's Beneficial Owner. If an entity issues bearer shares, the shareholder or owner of that entity is any person who holds the shares (on paper) at any given time. Dividends are paid against the presentation of paper shares, but the identity of the Beneficial Owner is not necessary revealed. Bearer shares allow the transfer of ownership by simply handing the shares to another person. If the Beneficial Owner controls an entity through bearer shares, it is very difficult to determine his identity.

The legal entities can be used to facilitate money laundering and other crimes because their true ownership can be hidden. The collection of beneficial ownership information about the

legal entity customers can provide law enforcement with key details about suspected criminals who use legal entity structures to conceal their illicit activity and assets.

The ultimate beneficial owner plays an important role regarding the transparency of the financial sector and the law enforcement efforts.

There are different approaches to ensure the transparency of the beneficial ownership, namely:

a) Registry Approach – requiring company registries to obtain and hold up-to-date information on beneficial ownership;

b) Existing Information Approach – using existing sources of information incl. financial institutions, company, land, property or other types of registries, other authorities (tax authorities, stock exchanges), commercial databases;

c) Company Approach – requiring companies themselves to obtain and hold up-to-date information on shareholders or members.

The countries are allowed to use one or more approaches to ensure the transparency of the beneficial ownership.

According to the FATF evaluations, the countries that are using a single approach are less effective in making sure that competent authority can obtain accurate and up-to-date BO information in a timely manner. Instead, a multi-pronged approach using several sources of information is often more effective in preventing the misuse of legal entities for criminal purposes and implementing measures that make the beneficial ownership of legal entities sufficiently transparent.

According to the 2018 FATF-Egmont report, increased sharing of relevant information and transaction records would benefit global efforts to improve the transparency of beneficial ownership.

Beneficial ownership legislation in Republic of Bulgaria

According to the Bulgarian Measures Against Money Laundering Act ('**MAMLA**') the beneficial owner *is:*

„a natural persons/s, who possess or control legal person or other legal formation and/or natural person/s on whose behalf, or for his expense a certain operation is performed or activity, and who meet at least one of the following conditions:

1. In relation or the cooperative legal person or other legal formations, the real owner is the person, who directly or indirectly possesses sufficient percentage of the assets, shares or rights to vote in this legal person, or another legal formation, including through holding assets of a bearer, or through control through other funds, with the exception of the cases of a company, whose assets are traded on a regulated market, which is subordinated to the requirement for announcement in compliance with the EU law or with equivalent international standards, providing adequate level of transparency in relation to ownership.

Indication for direct possession is present where a natural person/s has assets or share participation at least 25% of a legal person or other legal formation.

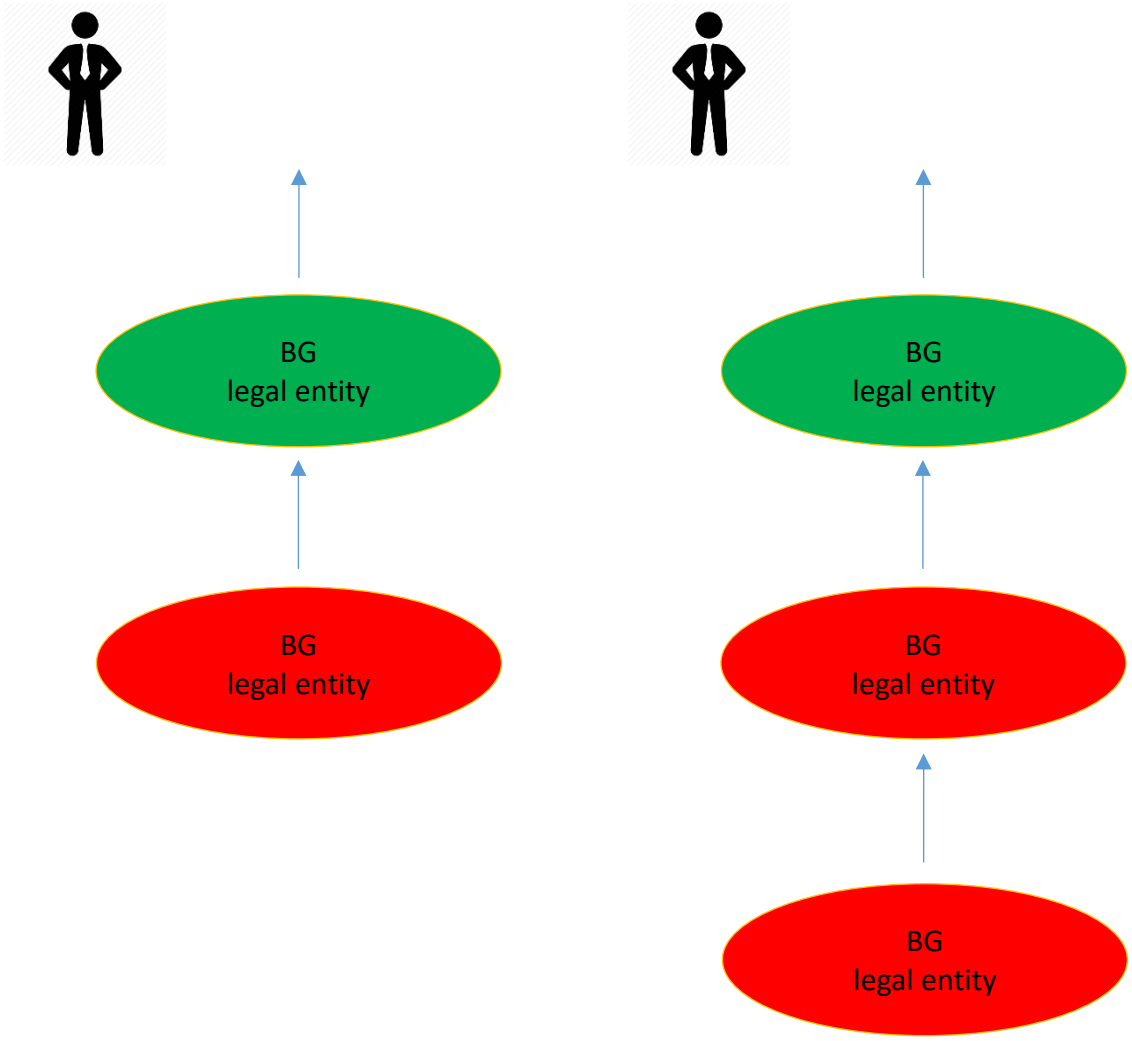
Indication of indirect possession is present, where at least 25% of the assets or share participation in a legal person or other legal formation belongs to a legal person or another legal formation, which is under the control of one and the same natural person/s or many legal persons and/or legal formation, which are under the control of the same natural person/s.
2. In relation to the trust ownership, including trusts and other similar foreign legal formations, established and existing under the law of the jurisdictions, admitting such forms of trust ownership, the real owner is:
a) the establisher;
b) the trust owner;
c) the keeper – if any;
d) the beneficiary or the class of beneficiaries, or
e) the person in whose major interest is created or is managed the trust ownership, where the natural person, who benefits from it is to be determined;
f) any other natural person, who manages control over trust ownership by direct or indirect possession or other means.
3. In relation to foundations and legal forms, similar to trust ownership – the natural person/s, who occupy positions, equivalent or similar to those, indicated in p. 2.
(2) Real ownership is not the natural person/s, who are nominal directors, secretaries, shareholders or owners of the capital or a legal person or another legal formation if another real owner is established.
(3) "Control" is the control in the meaning of § 1c of the Additional Provision of the Commerce Act, as well as any possibility, which without being indication for direct or indirect possession, givers opportunity for exercising a decisive influence over a legal person or another legal formation with decision taking for determining the staff of the management and control bodies, reformation of the legal person, termination of its activity and other issued of substantial significance about its activity.
(4) Indication for indirect control is exercising an end effective control over the legal person or another legal formation by exercising rights through third persons, including – but not only – provided under authorization, contract or another transaction, as well as through other legal forms, providing possibility for exercising influence through third persons.
(5) Where after all possible means have been exhausted and provided that there are no grounds for doubting, it is impossible to establish the real owner under Para. 1, or where there is doubt, that the established person/s are not the real owner, as real owner shall be considered the natural person, who fulfills the position of high risk official. The obliged persons keep documentation for the undertaken actions in view to establishing the real owner under Para. 1."

According to the MAMLA:

"The legal persons and other legal formations…, established on the Republic of Bulgaria, shall be obliged to receive, dispose of and provide in the cases, provided by the law, appropriate, exact and updated information about the natural persons, who are their real owners, including with detailed data about the rights, held by them."

When the obliged entities undertake measures for a complex checkup of the client in compliance with the requirements of MAMLA and the Rules on its implementation, the established on the Republic of Bulgaria legal entities and other legal formations, which step in

business relations or performed random operation or transaction with, or through them shall be obliged to produce to the obliged entities information about their beneficial owners, required



LEGEND:

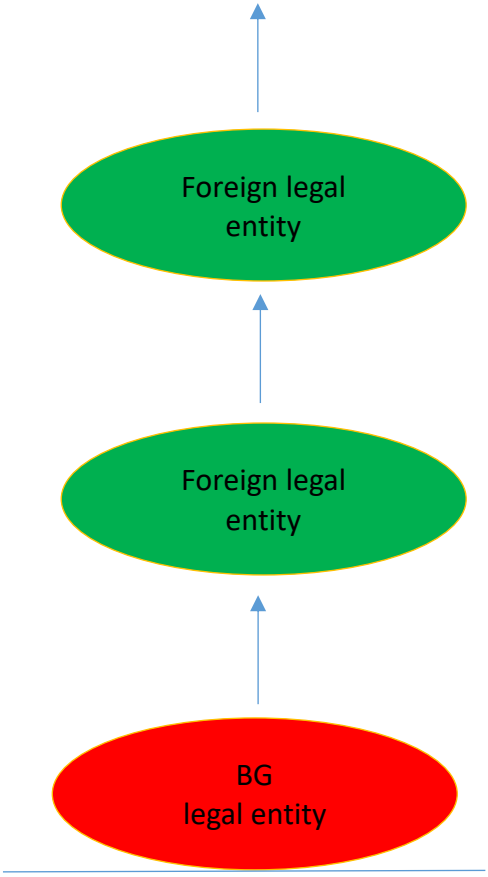
obligation for UBO disclosure

no obligation for UBO disclosure

Bulgarian or foreign individual

under MAMLA.

Figure BO disclosure obligation



The established in Bulgaria legal entities must have a “contact natural person” which have to be stated before the Bulgarian Commercial Register and Register for the non-profit legal entities. The contact person shall provide, upon request the information above to the Financial Intelligence Directorate of the National Security State Agency and to the competent bodies under this act with the term, defined by them.

The Bulgarian Commercial Register and Register for the non-profit legal entities is a public register and contains public information about the beneficial ownership and the natural contact person.

The obligation to state a contact person arises when no data for permanently residing person on the territory of Republic of Bulgaria is entered in the registration of the Bulgarian legal entity. The contact natural person must be permanently residing on the territory of the Republic of Bulgaria. The contact person provides his notary certified consent in order to be registered as a contact person of a legal entity.

The information for the beneficial owner and the contact person shall be entered in the registration files of the legal entity established on the territory of the Republic of Bulgaria.

The purpose of this is provisions is to ensure that competent authorities have timely access to adequate, accurate and up-to-date beneficial ownership information.

2.6. FATF RECOMMENDATIONS

The FATF Recommendations are the internationally endorsed global standards against money laundering and terrorist financing: they increase transparency and enable countries to successfully take action against illicit use of their financial system. They set out the principles for action and allow countries a measure of flexibility in implementing these principles according to their particular circumstances and constitutional frameworks.

Though not a binding international convention, many countries in the world have made a political commitment to combat money laundering by implementing the 40 Recommendations. Initially developed in 1990, the Recommendations were revised for the first time in 1996 to take into account changes in money laundering trends and to anticipate potential future threats.

The FATF Recommendations:

A. AML/CFT POLICIES AND COORDINATION

1. Assessing risks and applying a risk-based approach

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk-based measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions.

Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.

2. National cooperation and coordination

Countries should have national AML/CFT policies, informed by the risks identified, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies.

Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policy-making and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate and exchange information domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. This should include cooperation and coordination between relevant authorities to ensure the compatibility of AML/CFT requirements with Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation).

B. MONEY LAUNDERING AND CONFISCATION

3. Money laundering offence

Countries should criminalize money laundering on the basis of the Vienna Convention and the Palermo Convention. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences.

4. Confiscation and provisional measures

Countries should adopt measures similar to those set forth in the Vienna Convention, the Palermo Convention, and the Terrorist Financing Convention, including legislative measures, to enable their competent authorities to freeze or seize and confiscate the following, without prejudicing the rights of bona fide third parties: (a) property laundered, (b) proceeds from, or instrumentalities used in or intended for use in money laundering or predicate offences, (c) property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations, or (d) property of corresponding value.

Such measures should include the authority to: (a) identify, trace and evaluate property that is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries should consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction (non-conviction based confiscation), or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

C. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

5. Terrorist financing offence

Countries should criminalise terrorist financing on the basis of the Terrorist Financing Convention, and should criminalise not only the financing of terrorist acts but also the financing

of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences.

6. Targeted financial sanctions related to terrorism and terrorist financing

Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001).

7. Targeted financial sanctions related to proliferation

Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.

8. Non-profit organisations

Countries should review the adequacy of laws and regulations that relate to non-profit organisations which the country has identified as being vulnerable to terrorist financing abuse. Countries should apply focused and proportionate measures, in line with the risk-based approach, to such non-profit organisations to protect them from terrorist financing abuse, including:

i. by terrorist organisations posing as legitimate entities;
ii. by exploiting legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and
iii. by concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

D. PREVENTIVE MEASURES

9. Financial institution secrecy laws

Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

CUSTOMER DUE DILIGENCE AND RECORD-KEEPING

10. Customer due diligence

Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.

Financial institutions should be required to undertake customer due diligence (CDD) measures when:

i. establishing business relations;
ii. carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;
iii. there is a suspicion of money laundering or terrorist financing; or
iv. the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means.

The CDD measures to be taken are as follows:

a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.
b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.
c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above, but should determine the extent of such measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1.

Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with the applicable requirements under paragraphs (a) to (d) above (subject to appropriate modification of the extent of the measures on a risk-based approach), it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, although financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

11. Record-keeping

Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should be required to keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.

Financial institutions should be required by law to maintain records on transactions and information obtained through the CDD measures.

The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

ADDITIONAL MEASURES FOR SPECIFIC CUSTOMERS AND ACTIVITIES

12. Politically exposed persons

Financial institutions should be required, in relation to foreign politically exposed persons (PEPs) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:

a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;
b) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
c) take reasonable measures to establish the source of wealth and source of funds; and
d) conduct enhanced ongoing monitoring of the business relationship.

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organisation. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d).

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

13. Correspondent banking

Financial institutions should be required, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, to:

a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;
b) assess the respondent institution's AML/CFT controls;
c) obtain approval from senior management before establishing new correspondent relationships;
d) clearly understand the respective responsibilities of each institution; and
e) with respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.

Financial institutions should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks. Financial institutions should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

14. Money or value transfer services

Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTS) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions.

Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or the MVTS provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate. Countries should take measures to ensure that MVTS providers that use agents include them in their AML/CFT programmes and monitor them for compliance with these programmes.

15. New technologies

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

16. Wire transfers

Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.

Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measures.

Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing.

RELIANCE, CONTROLS AND FINANCIAL GROUPS

17. Reliance on third parties

Countries may permit financial institutions to rely on third parties to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10.

b) Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

c) The financial institution should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11.

d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

When a financial institution relies on a third party that is part of the same financial group, and (i) that group applies CDD and record-keeping requirements, in line with Recommendations 10, 11 and 12, and programmes against money laundering and terrorist financing, in accordance with Recommendation 18; and (ii) where the effective implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority, then relevant competent authorities may consider that the financial institution applies measures under (b) and (c) above through its group programme, and may decide that (d) is not a necessary precondition to reliance when higher country risk is adequately mitigated by the group AML/CFT policies.

18. Internal controls and foreign branches and subsidiaries

Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement groupwide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.

Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programmes against money laundering and terrorist financing.

19. Higher-risk countries

Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks.

Countries should be able to apply appropriate countermeasures when called upon to do so by the FATF. Countries should also be able to apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks.

REPORTING OF SUSPICIOUS TRANSACTIONS

20. Reporting of suspicious transactions

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).

21. Tipping-off and confidentiality

Financial institutions, their directors, officers and employees should be:

a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and

b) prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU. These provisions are not intended to inhibit information sharing under Recommendation 18.

DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

22. DNFBPs: customer due diligence

The customer due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, apply to designated non-financial businesses and professions (DNFBPs) in the following situations:

a) Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.

b) Real estate agents – when they are involved in transactions for their client concerning the buying and selling of real estate.

c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

d) Lawyers, notaries, other independent legal professionals and accountants – when they prepare for or carry out transactions for their client concerning the following activities:

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

e) Trust and company service providers – when they prepare for or carry out transactions for a client concerning the following activities:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;

- acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

23. DNFBPs: Other measures

The requirements set out in Recommendations 18 to 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d) of Recommendation 22. Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to in paragraph (e) of Recommendation 22.

E. TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS

24. Transparency and beneficial ownership of legal persons

Countries should take measures to prevent the misuse of legal persons for money laundering or terrorist financing. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares or bearer share warrants, or which allow nominee shareholders or nominee directors, should take effective measures to ensure that they are not misused for money laundering or terrorist financing. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

25. Transparency and beneficial ownership of legal arrangements

Countries should take measures to prevent the misuse of legal arrangements for money laundering or terrorist financing. In particular, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

F. POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES, AND OTHER INSTITUTIONAL MEASURES

REGULATION AND SUPERVISION

26. Regulation and supervision of financial institutions

Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities or financial supervisors should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a financial institution. Countries should not approve the establishment, or continued operation, of shell banks.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes, and which are also relevant to money laundering and terrorist financing, should apply in a similar manner for AML/CFT purposes. This should include applying consolidated group supervision for AML/CFT purposes.

Other financial institutions should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing, they should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements.

27. Powers of supervisors

Supervisors should have adequate powers to supervise or monitor, and ensure compliance by, financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose sanctions, in line with Recommendation 35, for failure to comply with such requirements. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution's license, where applicable.

28. Regulation and supervision of DNFBPs

Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary AML/CFT measures. At a minimum:

- casinos should be licensed;

- competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, holding a management function in, or being an operator of, a casino; and
- competent authorities should ensure that casinos are effectively supervised for compliance with AML/CFT requirements.

b) Countries should ensure that the other categories of DNFBPs are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. This should be performed on a risk-sensitive basis. This may be performed by (a) a supervisor or (b) by an appropriate self-regulatory body (SRB), provided that such a body can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

The supervisor or SRB should also (a) take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding or being the beneficial owner of a significant or controlling interest or holding a management function, e.g. through evaluating persons on the basis of a "fit and proper" test; and (b) have effective, proportionate, and dissuasive sanctions in line with Recommendation 35 available to deal with failure to comply with AML/CFT requirements.

OPERATIONAL AND LAW ENFORCEMENT

29. Financial intelligence units

Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

30. Responsibilities of law enforcement and investigative authorities

Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations within the framework of national AML/CFT policies. At least in all cases related to major proceeds-generating offences, these designated law enforcement authorities should develop a pro-active parallel financial investigation when pursuing money laundering, associated predicate offences and terrorist financing. This should include cases where the associated predicate offence occurs outside their jurisdictions. Countries should ensure that competent authorities have responsibility for expeditiously identifying, tracing and initiating actions to freeze and seize property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime. Countries should also make use, when necessary, of permanent or temporary multi-disciplinary groups specialised in financial or asset investigations. Countries should ensure that, when necessary, cooperative investigations with appropriate competent authorities in other countries take place.

31. Powers of law enforcement and investigative authorities

When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions, DNFBPs and other natural or legal persons, for the search of persons and premises, for taking witness statements, and for the seizure and obtaining of evidence.

Countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery. In addition, countries should have effective mechanisms in place to identify, in a timely manner, whether natural or legal persons hold or control accounts. They should also have mechanisms to ensure that competent authorities have a process to identify assets without prior notification to the owner. When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to ask for all relevant information held by the FIU.

32. Cash couriers

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including through a declaration system and/or disclosure system.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing, money laundering or predicate offences, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing, money laundering or predicate offences, countries should also adopt measures, including legislative ones consistent with Recommendation 4, which would enable the confiscation of such currency or instruments.

GENERAL REQUIREMENTS

33. Statistics

Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems. This should include statistics on the STRs received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for cooperation.

34. Guidance and feedback

The competent authorities, supervisors and SRBs should establish guidelines, and provide feedback, which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.

SANCTIONS

35. Sanctions

Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons covered by Recommendations 6, and 8 to 23, that fail to comply with AML/CFT requirements. Sanctions should be applicable not only to financial institutions and DNFBPs, but also to their directors and senior management.

G. INTERNATIONAL COOPERATION

36. International instruments

Countries should take immediate steps to become party to and implement fully the Vienna Convention, 1988; the Palermo Convention, 2000; the United Nations Convention against Corruption, 2003; and the Terrorist Financing Convention, 1999. Where applicable, countries are also encouraged to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001; the Inter-American Convention against Terrorism, 2002; and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 2005.

37. Mutual legal assistance

Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions, and related proceedings. Countries should have an adequate legal basis for providing assistance and, where appropriate, should have in place treaties, arrangements or other mechanisms to enhance cooperation. In particular, countries should:

a) Not prohibit, or place unreasonable or unduly restrictive conditions on, the provision of mutual legal assistance.
b) Ensure that they have clear and efficient processes for the timely prioritisation and execution of mutual legal assistance requests. Countries should use a central authority, or another established official mechanism, for effective transmission and execution of requests. To monitor progress on requests, a case management system should be maintained.
c) Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.
d) Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions or DNFBPs to maintain secrecy or confidentiality (except where

the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies).

e) Maintain the confidentiality of mutual legal assistance requests they receive and the information contained in them, subject to fundamental principles of domestic law, in order to protect the integrity of the investigation or inquiry. If the requested country cannot comply with the requirement of confidentiality, it should promptly inform the requesting country.

Countries should render mutual legal assistance, notwithstanding the absence of dual criminality, if the assistance does not involve coercive actions. Countries should consider adopting such measures as may be necessary to enable them to provide a wide scope of assistance in the absence of dual criminality.

Where dual criminality is required for mutual legal assistance, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Countries should ensure that, of the powers and investigative techniques required under Recommendation 31, and any other powers and investigative techniques available to their competent authorities:

a) all those relating to the production, search and seizure of information, documents or evidence (including financial records) from financial institutions or other persons, and the taking of witness statements; and

b) a broad range of other powers and investigative techniques;

are also available for use in response to requests for mutual legal assistance, and, if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

Countries should, when making mutual legal assistance requests, make best efforts to provide complete factual and legal information that will allow for timely and efficient execution of requests, including any need for urgency, and should send requests using expeditious means. Countries should, before sending requests, make best efforts to ascertain the legal requirements and formalities to obtain assistance.

The authorities responsible for mutual legal assistance (e.g. a Central Authority) should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

38. Mutual legal assistance: freezing and confiscation

Countries should ensure that they have the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered; proceeds from money laundering, predicate offences and terrorist financing; instrumentalities used in, or intended for use in, the commission of these offences; or property of corresponding value. This authority should include being able to respond to requests made on the basis of non-conviction-based confiscation proceedings and related provisional measures, unless this is inconsistent with fundamental principles of their domestic law. Countries should also have effective mechanisms for managing such property, instrumentalities or property of corresponding value, and arrangements for coordinating seizure and confiscation proceedings, which should include the sharing of confiscated assets.

39. Extradition

Countries should constructively and effectively execute extradition requests in relation to money laundering and terrorist financing, without undue delay. Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations. In particular, countries should:

a) ensure money laundering and terrorist financing are extraditable offences;
b) ensure that they have clear and efficient processes for the timely execution of extradition requests including prioritisation where appropriate. To monitor progress of requests a case management system should be maintained;
c) not place unreasonable or unduly restrictive conditions on the execution of requests; and
d) ensure they have an adequate legal framework for extradition.

Each country should either extradite its own nationals, or, where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case, without undue delay, to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Where dual criminality is required for extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms, such as allowing direct transmission of requests for provisional arrests between appropriate authorities, extraditing persons based only on warrants of arrests or judgments, or introducing a simplified extradition of consenting persons who waive formal extradition proceedings. The authorities responsible for extradition should be provided with

adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

40. Other forms of international cooperation

Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing cooperation. Countries should authorise their competent authorities to use the most efficient means to cooperate. Should a competent authority need bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), these should be negotiated and signed in a timely way with the widest range of foreign counterparts.

Competent authorities should use clear channels or mechanisms for the effective transmission and execution of requests for information or other types of assistance. Competent authorities should have clear and efficient processes for the prioritisation and timely execution of requests, and for safeguarding the information received.

2.7 DESCRIPTION OF THE BEST PRACTICES AGAINST MONEY LAUNDERING IN BULGARIA

Bulgaria has made significant progress in the area of anti-money laundering during the last decade, both in terms of institutional set-up and legislative efforts. At the same time investigating and proving money laundering in court remains challenging, in particular as it relates to higher echelons of power and politically exposed persons. This is confirmed by the small share of money laundering sentences, compared to other types of crimes.

The effective anti-money laundering measures depends not only on the legislative changes and the harmonization of norms with the international recommendations, but also on the manner in which these recommendations are implemented. It’s important the means in which it will be operated to comply with the requirements of the law. Also important, is the way in which the law will be applied/used on practice to be clear.

As a good practice in the anti-money laundering system we may point out the establishment of guides by the obliged entities on how to act in the implementation of anti-money laundering procedures. The guides may be an element of internal control rules or an independent part of the policy of the obliged entities to prevent money laundering.

Countering money laundering requires a holistic approach on multiple levels. Enhancing the overall capacity to investigate money laundering should be highlighted in this regard.

The risk of exposure of obliged entities regarding attempts at money laundering is very different in every single case. The risk is determined by qualitative and quantitative aspects which are closely related to the type of activity carried out by each obliged entity.

A risk analysis needs to be carried out to determine where the risks of money laundering and terrorist financing are greatest. The obliged entities and the countries must also identify the main weaknesses and address them accordingly. The Institutions must identify higher-risk users, products and services, including delivery channels and geographical regions.

List of the general risks is presented in the National Risk Assessment of Bulgaria from 2020 and includes:

- Money laundering of a wide range of predicate offenses committed abroad or domestically related to organized crime (drugs, human trafficking tax crimes such as tax evasion) through the use of the formal financial system and the widespread use of funds in cash;
- Money laundering of money acquired through corruption (including property acquired through misappropriation of funds / fraud in public procurement with EU funds) through complex money laundering schemes inside or outside the country with the help of "professional washes" and subsequent integration the funds in financial instruments abroad and in legal entities and real estate in the country;
- Money laundering from tax crimes (avoidance of tax liability and VAT frauds) through the use of counterfeiters, local and foreign legal entities in complex layering schemes and with the help of "professional washers";
- Integration of significant "laundered assets" in the construction and real estate investments by local and foreign entities in the context of a significant share of the gray economy;
- Money laundering from predicate crimes, committed abroad through non-banking investment intermediaries in Bulgaria, as well as cases of unregulated trading in financial instruments;
- Money laundering from tax crimes (avoidance of tax evasion and VAT frauds) in the field of food and fuel trade through the use of hollow companies and nominal owners, aided by the corrupt environment and the "gray economy";
- Laundering of funds obtained from computer frauds and „social engineering" frauds committed by small or medium-sized organized crime groups (**OCGs**) who use the territory of the country to stratify funds;
- The possible involvement of professionals and obliged entities under the MAMLA, facilitated by vulnerabilities related to the rules for admission to the market (e.g. registration / licensing) and the selection of their employees, as a major risk contributing to the functioning of organized crime and contributes to the level of most of the above risks.
- And some high-risk terrorist financing events as:
- The use of cash transfer services, unregulated informal transfer services for the transfer of funds potentially related to terrorist financing, which is also facilitated by migrant communities, further heavily influenced by the cash and gray economy;
- The potential risk (limited) of diversion of funds earmarked for the activities of non-profit legal entities (**NGOs**) or for religious activities in Bulgaria to finance terrorism.

In the process of analyzing the risks of money laundering and terrorist financing, it is crucial to reach a broad understanding of why money laundering and terrorist financing occur. Money laundering and terrorist financing acts are being carried out to facilitate crime and terrorism more broadly. The criminals make great efforts to transfer illegally acquired money and other assets to replace, conceal, or mask the true nature and source of those funds.

The consequences of this illegal activities often occur at national or international level, but it also affects regional, local and individual levels. The impacts and harms can be further categorized into types such as physical, social, environmental, economic and structural. The money laundering and terrorist financing activities also damage the country's national security and reputation, and have a direct and indirect impact on the national economy.

The strict implementation of the procedures set out in the law makes it possible to effectively combat money laundering in any country that has adopted the regulation proposed by international organizations. While applying these standards and rules, each country must adapt them to the characteristic environment in a way that ensures their actual functioning. It is their effective functioning that builds up the good practices.

Due Diligence

The due diligence procedures main goals are to provide traceable customer footprints/marks for possible investigation by competent authorities and to make it more difficult for criminals to use the financial system to launder their illegally acquired money.

Customer identification means identifying and verifying the customer's identity through the use of reliable written and unwritten sources of information. The obliged entities must collect enough information to ensure the identity of each new customer. All obliged entities must create and implement written rules for identification of clients which are part of their money laundering prevention program. The obliged entities must introduce customer identification program that is best suited to their vulnerability to money laundering and terrorist financing.

The due diligence measures are covered by the application of the risk approach. In order to adopt appropriate measure to identify and asses the money laundering risks, the obliged entities must carry out analysis of the risk of money laundering to which they are exposed.

The relative weight to be assigned to each category when assessing the overall risk of money laundering and terrorism financing will vary depending on the obliged entity due to the size, sophistication, location and nature and scope of the services offered. Based on their individual practices and judgments, the obliged entities will need to independently assess the weight given to each risk factor.

Important component in the development and implementation of a framework risk is to determine the potential for money laundering or terrorism financing risk posed by a customer. Customers range from natural persons, associations, limited liability companies, companies with multiple members or members of multinational corporations. Given this spectrum of customers, the obliged entities must determine whether a particular customer poses a greater

risk and, if so, the level of that risk and whether the application of any mitigating factors influence that assessment.

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

- Politically exposed persons (**PEPs**) are individuals who are or have been entrusted with prominent public functions domestically or by a foreign country. If the obliged entity carries out a transaction for a customer who is PEP or owned by the PEP, they are required to perform a higher and more detailed form of due diligence;
- Customers who carry out their business relationship or request services under unusual or unconventional circumstances;
- Customers where the structure or nature of the entity or relationship makes it difficult to identify in a timely manner the true final beneficiary or those exercising control;
- Customer legal person that operates a substantial part of their business or has significant subsidiaries in countries that may have a greater geographical risk;
- Cash-intensive business customers (brokers, casinos, betting shops, money service business, etc.);
- Charities and other non-profit organisations that are not subject to supervision or surveillance by designated competent authorities or self-regulatory bodies;
- Customers who appear to be acting according to another person's instructions without revealing this fact, and who denies to disclose the information when required;
- Customers who avoid face-to-face meetings or provide intermittent instructions without legitimate reasons and who are otherwise elusive or very difficult to reach;
- Customers who have no address, or multiple addresses without legitimate reasons;
- Customers who change their settlement or execution instructions without a proper explanation;
- Customers who change their means of payment for a transaction at the last moment and without justification;
- Etc.

A general risk assessment should also include assessing the potential risks presented by the services offered by the obliged entities, taking into account the different services provided by them. The context of the services offered is always fundamental to a risk-based approach. Any of the above factors alone cannot constitute a high-risk circumstance, but the factors should be considered jointly.

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

Gathering and keeping of information

The gathering and the keeping of information is an essential part of the whole anti-money laundering regime and many of these requirements could not be fulfilled without it. The obliged entities must be able to provide the necessary information for their clients upon request.

The obliged entities must keep for period of 5 years all collected and prepared under the money laundering legislation documents, data and information.

The obliged entities must keep the following documentation for use in any investigation or analysis by the competent authorities of possible money laundering or terrorism financing case:

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

The filing system must ensure adequate management and availability of the documentation, both in internal control purposes and for the purposes of timely and formal attention to the requirements of the authorities.

Reporting suspicious transactions

This obligation implies that if the obliged entity suspects or has reasonable grounds to suspect that the funds are result of criminal activity, or are related to terrorist financing, they must report it promptly to the FIU.

When there is a notification about suspicion for money laundering and/or suspicion for funds of criminal nature, the director of Financial Intelligence Directorate of the National Security State Agency may stop with a written order a certain operation or transaction for the term of 5 working days, starting from the day, following the day of issuance of the order. The goal here is analysis to be performed from the competent authorities in order to confirm the suspicion and the result to be disclosed.

The fact that someone is suspected of money laundering, as well as information on the basis of which this conclusion is made, should be strictly limited.

Education and training of the employees

The provision of training for the employees about the new standards and requirements for the combating of money laundering and about criteria for suspicious of money laundering clients and transactions is a key aspect in the counteracting to the money laundering practices.

A key aspect of counteracting the money laundering is the provision of training on new standards and requirements for combating money laundering and learning about criteria for suspicious money laundering.

The training of the employees is a part of the internal organization and control rules of the obliged entities. The trainings should be carried out on a regular basis to keep employees informed of the latest developments in this field. The number of these trainings depends on the activities of the obliged entity and whether or not it is more vulnerable to being involved in money laundering schemes.

Practices of Customs, Law Enforcement Bodies, FIU, Tax Authorities and Banking Supervisors to identify suspected money laundering activities. Sharing with local and foreign partner services and taking action.

Customs

Most of the Customs services indicate that they use risk indicators or other forms of risk analysis to identify activities related to potential money laundering.

Customs services have training programs in place, but virtually everyone in Customs agrees on the need for better training and understanding on money laundering techniques and procedures.

One of the most effective means of analyzing and investigating suspicious activities, through the prism of the Customs, is to have in place systems that monitor daily imports and exports between
countries.

Law Enforcement Bodies

The information used by the Law Enforcement Bodies for analyzes is obtained from the FIU, Customs, Financial Institutions, Banking and Tax authorities. In a lot of the cases, this type of information is the reason for investigation.

Public political figures and other public figures

The status of a political person does not in itself mean that an individual is corrupt or involved in any kind of corruption scheme. Nevertheless, the threat of money laundering by public political figures and other public figures - both foreign and local - through officials must be met with understanding and action against the potential money laundering risks associated with these clients and transactions.

According to FATF reports, the public political figures might try to “launder” not only money from bribe, corruption and other directly corruption-related proceeds, but there may also be diversion of funds or outright theft of state assets or funds by political parties and unions, as well as tax fraud. The political figures from countries or regions with high corruption levels represents the highest risk for the occurrence of money laundering.

Business relationships with political figures pose increased risks due to the ability of individuals in such positions to abuse their power, or to influence personal favors and benefits or personal favors or benefits to their family or close associates. Such individuals may also use family members or close associates to conceal capital and assets that have been misappropriated as a result of abuse of office. The political figures may also use their power and influence to gain representation and/or access to, or control over, legal entities for such purposes.

The risk varies depending on various factors, including the country of the political figure, the specific production/sector and the products and services used. The risk will also change depending on factors such as the nature of the position and the nature/purpose of the service.

Money laundering and financing terrorism is a topic of discussion not only in the European Union and his institutions but also in the Member States. The European Union adopts legal acts for prevention of money laundering and terrorist financing permanently.

II. METHODOLOGIES FOR ASSESSMENT OF MARKET PRICES

It has been argued in the science community that transfer price-based capital flight and tax evasion are variants of money laundering in nature to the extent that they all enable the apparently legal ownership of the property shifted illegally[1].

In order to prevent and uncover activities of such kind one should use different methods for assessing the market prices.

The most prevalent and widely used methods are the ones established by the OECD in the Transfer
Pricing Guidelines for Multinational Enterprises and Tax Administrations. Although the legal status of the Guidelines varies from one state to another, the Guidance has generally been accepted by tax authorities as a basis for compliance with the arm's length principle. In addition, the OECD Guidelines integrate the extensive know-how of Member States and balances the different interests of these jurisdictions.

The OECD Guidelines require taxable profits or allowable losses to be calculated as if transactions between associated enterprises had been conducted on arm's length terms. The OECD Guidelines describe several different methods that taxpayers can use to assess whether related party transactions produce arm's length results. The methods can be classified into two general categories:

1) Traditional (transaction based) methods:
   - Comparable Uncontrolled Price ("CUP") method;
   - Resale Price method ("RPM"); and
   - Cost Plus method;
2) Other (profit based) methods:
   - Profit Split method; and

[1] Zeng-an, Gao & Li-fang, Weng. (2006). Transfer Price-based Money Laundering in International Trade. Proceedings of 2006 International Conference on Management Science and Engineering, ICMSE'06 (13th). 1128 - 1132. 10.1109/ICMSE.2006.314201.

- Transactional Net Margin method ("TNMM").

While there is no clear hierarchy of methods in the OECD Guidelines, there is a preference towards transactional methods over profit based methods, and within the transaction based methods there is a preference for the CUP method. However, the OECD Guidelines recognize that no one method is applicable to every case, rather, the method used should be that which, given the specific circumstances, provides the most reliable measure of an arm's length result. Moreover, the OECD

Guidelines state that taxpayers retain the freedom to apply other, non-specified methods, provided that the derived result satisfies the arm's length principle.
The application of each of the three transactional based methods relies on the identification of uncontrolled transactions for comparison against the controlled transaction.

1. Comparable uncontrolled price method (CUP)

The CUP method compares the amounts charged in controlled transactions with amounts charged in comparable third party transactions. Comparable transactions may be between two third parties (i.e., an external CUP) or between one of the related parties and a third party (i.e., an internal CUP).

In practice, the CUP method involves direct comparison of the nominal prices used by related parties in the controlled transaction with their market equivalents (uncontrolled transactions). As a result, high level of comparability in terms of the transaction subject, functional profile of the parties, contractual terms, market conditions, etc., is required in order to apply it. The transactions are considered comparable if there are no differences between them that could significantly affect the prices, or the effect of such differences can be eliminated by appropriate adjustments.

A potentially comparable transaction would involve one of the following:

- Extension of a loan to the particular entity by an unrelated party under similar circumstances, terms and conditions;

- Extension of a loan to an unrelated party by the particular entity under similar circumstances, terms and conditions;

- Identification of transactional data on the extension of loans between third parties (uncontrolled entities), under similar circumstances, terms and conditions.

For the purposes of CUP an uncontrolled transaction is comparable to a controlled transaction (i.e. it is a comparable uncontrolled transaction) if one of two conditions is met:

- None of the differences (if any) between the transactions being compared or between the enterprises undertaking those transactions could materially affect the price in the open market; or,

- Reasonably accurate adjustments can be made to eliminate the material effects of such differences.

The CUP method is preferred over all other methods as the most direct and reliable way of applying the arm's length principle when the subject of a controlled and comparable uncontrolled transaction is the same product or service and the persons being compared perform the same functions. Unlike other methods, the method of comparable uncontrolled

prices directly examines the market price, not the rate of gross or net profit. Therefore, using the method requires near-perfect comparability between transactions. It is this requirement of similarity that makes it difficult to put into practice. The CUP method is often used in the case of intangible goods transactions, especially in the area of granting trademark rights to cosmetics and luxury goods, as well as in franchise agreements.

The specifics of the method require first of all to consider the characteristics of the product or service as a leading pricing factor. To this end, product comparability analysis shall include the following components:

- In the case of delivery of goods – the physical properties of the product, quality, durability, materials and technology used, intangible goods related to the goods, etc.;

- In the case of provision of services – the type, nature and extent of the services used, intangibles associated with the service, etc.;

- In the case of the provision of intangible goods – type (patent, trademark, know-how, etc.), duration and degree of protection, uniqueness, expected benefits from the use of the goods, etc.

In order to achieve greater reliability of the results of the CUP method, when analyzing the comparability of a controlled and uncontrolled transaction, the effect on price by complex economic functions must be taken into account instead of only comparing product similarity. In this regard, the following pricing factors are also taken into account when implementing the CUP method:

- Terms of the deal - quantity, respectively discounts on quantity, terms of delivery, allocation of risks on the transaction, (currency risk, credit risk, risk of loss of property, etc.), right to update and modify the provided product, negotiation moment, terms, provision of additional services such as installation and warranty service;

- Market conditions - geographical market in which the product or service is provided, market size, market level (wholesale or retail market), market share of the product or service, development of competition in relation to the product or service, availability of substitute products, phase of the business cycle of the market, level of inflation;

- Business strategies - entering a new market, expanding market share in an existing market, developing and marketing a new product, withdrawing from a market.

The requirement for comparability is crucial for the reliable application of the comparable uncontrolled price method. The deals in question should not be significantly different from each other as the difference could have an impact on the price of the transaction, i. e. the proper selection of comparable transactions is a key condition for the application of the method.

If it is not possible to establish fully comparable transactions, it is permissible to adjust the differences between the controlled and the uncontrolled transactions in order to obtain a reliable market price. The following adjustments are possible:

- Adjustments reflecting the incorporation in the product/service of trademarks or other intangible goods;
- Adjustments to working capital needs;
- Adjustments in case of an excessive number or insufficient number of employees;
- Adjustments for differences in accounting;
- Adjustments for differences related to sales or contractual terms.

2. Other traditional methods

Whenever the CUP method cannot be applied due to lack of information on comparable transactions, the use of other traditional methods - Resale Price method (RPM) or Cost Plus method (CPM) should be considered. For that purpose, functional profile of both parties to the controlled transaction must comply with functional profile of independent entities in comparable transactions. Unlike in the case of the CUP method, complete compatibility of transaction subject is not a prerequisite.

The RPM takes the price at which a product is resold to an independent third party and reduces this resale price by an appropriate gross margin, representing the amount out of which the reseller would seek to cover its selling and operating expenses and, in the light of its functions and risks, make an appropriate profit. It is generally accepted that the RPM is appropriate and applicable where an entity performs distribution functions (i.e., where there is little or no value added by the reseller prior to the resale of the goods acquired from related parties).

The RPM is most often used for distributors that resell physical products without altering them or adding substantial value to them. Therefore, the RPM is considered an inappropriate methodology to verify the arm’s length nature of pricing policy in the covered transactions.

On the other hand, the Cost Plus method is typically used in assessing an arm’s length price for manufacturers selling to related parties and for the provision of services to related parties. It compares the profit earned by the related party in a controlled transaction to the profit earned

by third parties in an uncontrolled transaction by reference to an appropriate cost plus mark-up to the costs incurred by a producer or a supplier of services. The level of mark-up on costs should be set, where possible, by reference to levels that exist in the open market between independent parties.

3. Transactional profit methods

The traditional transaction methods discussed above are the most direct means of establishing whether conditions in the commercial and financial relations between related parties are at arm's length. However, there may be some practical difficulties in their application. If comparable transactions cannot be identified or if there are material differences between the tested transactions and those of the independent comparable companies, then the traditional transaction methods can become less reliable than other methods. In those circumstances, it may be appropriate to use other, profit based methods.

The two methods described in the OECD Guidelines, and their applicability, are discussed below.

4. Transactional profit split method

Under the profit split method, a division of total profits between related parties is derived on the basis of what independent enterprises would have expected to make from comparable transactions. The profit split method is often appropriate for transactions that are so interrelated that they cannot be evaluated on a separate basis. Such situations might arise in circumstances where both parties in a controlled transaction jointly contribute to the creation of an intangible asset, and therefore, both earn a residual income as a result of the intangible. In these cases, the OECD Guidelines suggest that third parties might form a joint venture or partnership and agree to a form of profit split amongst them. The profits should be split on an economically valid basis that reflects the functions and risks of each of the parties involved.

As per the OECD Guidelines, the profit split is usually applied when either: transactions are extremely interrelated such that they cannot be evaluated on a separate basis or when it is difficult to identify appropriate operating expenses arising from the transactions so that costs cannot be allocated between the related parties.

5. Transactional net margin method

According to the OECD Guidelines: "the transactional net margin method examines the net profit margin relative to an appropriate base (e.g., costs, sales, assets) that a taxpayer realizes from a controlled transaction (or transactions that are appropriate to aggregate under the principles of Chapter I)". Thus, the TNMM operates in a manner similar to the Cost Plus method and the RPM. However, unlike the transactional methods, the TNMM does not require highly detailed price or gross margin transactional information, only net margin information.

Essentially, the TNMM is a profit based method that tests the arm's length nature of related party transactions by comparing the net margin results of related party transactions with the net

margin results of third-party companies engaged in similar functions and incurring similar business risks.

III. RISK ASSESSMENT METHODOLOGIES

1. Risk factors

The main risk factors are:

Groups of subjects potentially involved in money laundering activities, are:

- *The local natural persons* represent the widest group of subjects, involved in potential money laundering activities. The scenarios of highest risk, which include natural persons, refer to the usage of nominees (hidden ownership) in the schemes of money laundering, which is the main method (modusoperandi), used by the organized crime groups;

- *The local companies and non-profit organizations* represent the second biggest group of subjects, involved in potential money laundering activities, as in these cases the average amount of the sums is much higher than in the natural persons case;

- *Foreign companies and non-profit organizations* (mostly related to international money laundering, mostly computer scams);

- *Local important political personalities*;

- *Foreign important political personalities*. Under the National Risk Assessment, main risk scenario regarding the foreign political personalities and foreign natural persons is the usage of related to them persons for laundering of gained by corruption means by their investment in liquid actives, or, in particular cases, by their participation in privatization, as well as in a Program for citizenship against investment.

Risk clients are:

- Representatives and authorized natural persons or a *companies and non-profit organizations*, representing identity and legal documents whose authenticity is in doubt;

- All natural and legal persons, groups and organizations *appearing in the list under Art. 5 of the Measures Against Financing Of Terrorism Act*, which list is adopted, supplemented and amended by the Council of Ministers, to which the measures against the financing of terrorism are applied, including:

    - Individuals, legal entities, groups and entities designated by the UN Security Council as having links to terrorism or subject to terrorism sanctions by a UN Security Council resolution;

- Clients against whom criminal proceedings have been instituted for terrorism, terrorist financing, formation, leadership or membership in an organized criminal group that aims to commit terrorism or terrorist financing, preparation for terrorism or threat to commit terrorism within the meaning of the Criminal Code;

❖ Clients designated by the competent authorities of another country of the European Union;

❖ Clients included in the list of persons under Art. 3 of the Law on Information on Non-performing Loans;

❖ Clients for whom it is public knowledge that they have been criminally exposed;

❖ Clients from countries with offshore status or designated as tax havens;

❖ Clients from countries that do not implement the FATF recommendations;

❖ Customers who refuse to provide information about their identification;

❖ Clients presenting personal documents in which there are no basic details to fully identify him;

❖ Clients identifying with foreign identity documents, the authenticity of which is difficult to verify;

❖ Customers, indicating as an address the address of a third party or address for correspondence, which is a mailbox, without a logical explanation;

❖ Clients proposing that incorrect documents be drawn up during operations or that they be formalized in a manner different from the actual relations between the parties;

❖ Clients performing operations and transactions through a branch of a bank, without their registered office or activity on the territory of this branch;

❖ Clients from countries with offshore status or designated as tax havens;

❖ Prominent political figures, according to Art. 36 of the MAMLA.

According to Art. 36 of the MAMLA, prominent political figures are natural persons who perform or have been entrusted with the following important public functions:

❖ Heads of State, Heads of Government, Ministers and Deputy Ministers or Assistant Ministers;

❖ Members of parliaments or other legislative bodies;

❖ Members of constitutional courts, supreme courts or other supreme bodies of the judiciary, whose decisions are not subject to subsequent appeal except in exceptional circumstances;

- Members of the National Audit Office;
- Members of management bodies of central banks;
- Ambassadors and heads of diplomatic missions;
- Senior officers of the armed forces;
- Members of administrative, management or supervisory bodies of state enterprises and commercial companies with sole owner - the state;
- Mayors and deputy mayors of municipalities, mayors and deputy mayors of regions and chairmen of municipal councils;
- Members of the governing bodies of political parties;
- Heads and deputy heads of international organizations, members of management or supervisory bodies in international organizations or persons performing an equivalent function in such organizations.

Risk countries and geographical zones

Risk countries and geographical areas are offshore areas, countries that do not implement the recommendations of the FATF (Financial Action Task Force), countries that seek refuge from banking secrecy, as well as all countries outside the European Union, respectively. customers from these territories.

According to the current FATF list, high-risk third countries are: Afghanistan, American Samoa, Bahamas, Barbados, Botswana, Cambodia, Ghana, Iraq, Jamaica, Mauritius, Mongolia, Myanmar/ Burma, Nicaragua, Pakistan, Panama, Syria, Trinidad and Tobago, Uganda, Vanuatu, Yemen, Zimbabwe Democratic People's Republic of Korea, Ethiopia, Ghana, Guam, Iran, Iraq, Libya, Nigeria, Pakistan, Panama, Puerto Rico, Samoa , Sri Lanka, Syria, Trinidad and Tobago, Tunisia, the US Virgin Islands.

Risky operations

The characteristics that classify an operation as suspicious are:

- unusual operating conditions;
- operation with a risk client;
- lack of economic and legal justification;
- transaction with a client from or for a country on the list of countries at risk;
- client is a citizen of a dubious country or a person under Art. 36 of the LMML;
- operations based on cash or financed with anonymous electronic money, including electronic money;
- other doubtful facts.

Risk sectors of activity

The obligated entities should exercise due diligence in applying its Measures for prevention of money laundering in relation to the risk sectors of activity, namely:

• Financial sector (cash payments, formal financial system);

• The banking sector (cross-border inspections and cash withdrawals);

• In the sector of investments in financial instruments (the highest risk are investment intermediaries operating online trading platforms);

• Remittance services sector (remittances available);

• The electronic money sector;

• The insurance sector;

• The currency exchange sector;

• Economic sectors (fuels, coal mining, wholesale and retail trade, transport, real estate and agriculture);

• Terrorist financing.

Risky services

According to the National Risk Assessment, high-risk sectors include persons who provide legal advice by profession and persons who provide accounting services and / or tax advice by profession, in terms of regulation and their role in complex business and real estate transactions, the establishment and management of companies, as well as the facilitation of international transactions, incl. with offshore jurisdictions. Froneri does not provide any of the above services.
Risky events

The main risk events identified by the National Risk Assessment include:

• Money laundering from a wide range of predicate offenses committed abroad or in the country related to organized crime (mainly drugs, trafficking in human beings and tax crimes such as tax evasion) through the use of the formal financial system and the widespread use of cash;

• Money laundering acquired through corruption (including property acquired through misappropriation / fraud through public procurement with EU funds) through complex money laundering schemes in the country or abroad with the help of "professional money launderers"

and subsequent integration of funds in financial instruments abroad and in legal entities and real estate in the country;

• Money laundering from tax crimes (avoiding the establishment of tax liabilities and VAT fraud) through the use of proxies, local and foreign legal entities in complex stratification schemes and with the help of "professional laundries";

• Integration by local and foreign persons of significant amounts of “laundered funds” in the sector of construction and real estate investments in the context of the significant share of the gray economy;

• Money laundering from predicate offenses committed abroad through non-bank investment intermediaries in Bulgaria, as well as cases of unregulated trading in financial instruments;

• Laundering of funds obtained from tax crimes (avoidance of tax liabilities and VAT fraud) in the field of food and fuel trade through the use of hollow companies and nominal owners, supported by the corrupt environment and the gray ‘economy‘;

• Laundering of funds obtained from computer fraud and ‘social engineering‘ fraud committed by small or medium-sized organized criminal groups (OCGs) that use the territory of the country to stratify funds;

• The possible involvement of professionals and obligated entities under the Anti-Money Laundering Measures Act (LMML), facilitated by vulnerabilities related to market access rules (eg registration / licensing) and the selection of their employees, as a major risk that supports the functioning of organized crime and contributes to the level of most of the above risks.

Doubtful sources of money (property, ownership) are offshore areas, countries that do not apply the recommendations of the FATF, countries that are shelters of bank secrecy.

Illegal sources through which it can be formed and used as a source of terrorist income and property are:

• Drug production, smuggling and trafficking;

• Theft of personal documents for profit;

• Cybercrime through fraud with credit cards, insurance, social security cards and others;
• Counterfeiting of retail chains, including consumer items such as branded clothing, jewelry, fashion accessories and household products;

• International cigarette smuggling;

• Alternative systems for money transfers and unlicensed currency transfers and others

2. Suspicious transactions, transactions and customers, aimed at financing terrorism

'Terrorist financing' within the meaning of the LFTA is the direct or indirect, illegal and intentional provision and / or collection of funds, financial assets or other property and / or provision of financial services with the intention of using them or with the knowledge that will be used, in whole or in part, to commit terrorism within the meaning of the Penal Code.

The possible measures in counteraction to terrorism and in implementation of the LFTA are blocking of funds, financial assets and other property; prohibition on the provision of financial services, cash, financial assets or other property.

When performing a risk assessment, the obligated entities will have to take into account the following factors:

Intrinsic Threat Factors: The territory of the Republic of Bulgaria is part of an established trade and transport corridor between the Middle East and Europe, known as the "Balkan Route". The route is used for criminal purposes, incl. the smuggling of goods and trafficking in drugs, human beings, weapons, as well as goods and means of legal and illegal origin passing through the route to or from Central / Western Europe or Northeastern Europe and Asia. As a result of Bulgaria's geographical position, the country's territory is in transit for various predicate offenses, the perpetrators of which abuse a number of financial and non-financial sectors. The "Balkan route" also serves as a corridor for the transportation across the border of large sums of cash to and from Europe.

A Contextual factors: Most risks of money laundering and terrorist financing are exacerbated by contextual factors, including the significant size of the informal economy, the levels of corruption identified and the potential effectiveness issues of some of the competent national authorities. Another contextual factor is related to the characteristics of the population and the large percentage of people below the poverty line. This factor makes possible the systematic use of surrogates in money laundering schemes and is a factor of inherent vulnerability in the context of terrorist financing. The large percentage of Bulgarians who emigrated to other countries is also a factor of contextual importance for the easier spread of cross-border crime links with Bulgaria.

3. Comparison of AML Measures and National Risk Assessments in Bulgaria, Malta and The Kingdom of Netherlands

AML Measures in Bulgaria

The Bulgarian legislation establishes several measures aiming to prevent the use of the financial system for the purpose of money laundering. They are as follows:

a) complex inspection of clients;

b) collection and preparation of documents and other information required by the regulations established in the Bulgarian Anti-Money Laundering Measures Act;

c) storage of the documents, data and information collected and prepared for the purposes of the Anti-Money Laundering Measures Act;

d) assessment of the risk of money laundering and terrorist financing;

e) disclosure of information regarding suspicious operations, transactions and clients;

f) disclosure of other information for the purposes of the Anti-Money Laundering Measures Act;

g) control over the activity of the subjects obligated to report under the Anti-Money Laundering Measures Act;

h) exchange of information at national level, as well as exchange of information and interaction between the Financial Intelligence Directorate of the State Agency for National Security, the financial intelligence units of other countries and jurisdictions, as well as with the competent authorities and organizations in the respective field of other countries.

Complex inspection of clients

The complex inspection of the clients includes the following steps:

- identification of clients and verification of their identification on the basis of documents, data or information obtained from reliable and independent sources;

- identification of the beneficial owner and undertaking of appropriate actions for verification of his identification in a way, which gives the person obligated to take the anti-money laundering measures sufficient grounds to accept that the beneficial owner has been established;

- collection of information and assessment of the purpose and nature of the business relations, which have been established or are to be established with the client;

- clarification of the origin of the funds;

- current monitoring of the established business relationships and verification of the transactions and operations performed during the entire duration of these relationships, to what extent they correspond to the risk profile of the client and to the information about the client and / or collected during the application of the above mentioned measures, as well as timely updating of the collected documents, data and information.

The persons obliged to report apply the measures for complex inspection of the client at:

- establishment of business relations, including when opening an account, when with the opening of the account business relations are established;

- performing a random operation or concluding a random transaction of a value equal to or exceeding the BGN equivalent of EUR 15,000 or their equivalent in another currency, regardless of whether the operation or transaction was carried out through one operation or through several related operations;

- performing a random operation or concluding a random transaction of a value equal to or exceeding the BGN equivalent of EUR 5,000 or their equivalent in another currency, when the payment is made in cash, regardless of whether the operation or transaction is performed through one operation or through several related operations;

- performing a random operation or concluding a random transaction, which represents a transfer of funds according to art. 3, point 9 of Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) № 1781/2006 (OB, L 141 / 1 of 5 June 2015), at a value equal to or exceeding the BGN equivalent of EUR 1,000 or their equivalent in another currency.

In the cases when due to the nature of the accidental operation or transaction its value cannot be determined at the moment of its execution, the measures for complex inspection of the client shall be applied not later than the moment when the value of the operation or transaction be determined if it is equal to or greater than:

- the BGN equivalent of EUR 15,000 or their equivalent in another currency, regardless of the manner in which the payment is made and whether the operation or transaction was carried out through one operation or through several related operations;

- the BGN equivalent of EUR 5,000 or their equivalent in another currency, when the payment is made in cash, regardless of whether the operation or transaction has been carried out through one operation or through several related operations.

When a higher risk has been established, the persons obliged to report shall apply the following measures, and may take into account the scope and the degree of their application with the identified risk:

- apply clear internal procedures, including determination of the activities, internal rules for reporting, control and distribution of the functions in the organization, inspection of key employees for existence of negative public information or possible, procedures for allocation of funds, full control over the used bank accounts and financial instruments, monitoring of the activity of branches or related non-profit legal entities;

- apply procedures for control or cooperation with partner organizations, documenting the responsibilities in writing, receiving feedback on the use of funds and resources and ensuring the knowledge of the partner organizations of the beneficiaries of their activities;

- identify donors and beneficiaries by collecting the most complete information possible, allowing unambiguous identification, including in relation to controllers, without significantly impeding the activities of the organization, and if necessary, can use the methods and means of comprehensive verification;

- store all received funds and grant funds to beneficiaries, when this does not significantly impede the activity of the organization;

- check the donors and the beneficiaries, the partner non-profit legal entities for the existence of negative public information.

The organizers of gambling games within the meaning of the Bulgarian Gambling Act, who have received a license from the State Gambling Commission to organize their permitted gambling games shall apply the measures for complex inspection of the client at:

- the entry in the obligatory special register for visitors in a casino;

- the payment of profits and / or the placing of bets of a total value equal to or exceeding the BGN equivalent of EUR 2,000 or their equivalent in another currency, regardless of whether the operation or transaction has been carried out through one operation or through several related operations;

- purchase, exchange or redemption of tokens to confirm the profit of a total value equal to or exceeding the BGN equivalent of EUR 2,000 or their equivalent in another currency, regardless of whether the operation or transaction was carried out through one operation or through several related operations.

In the cases when due to the nature of the operation or transaction its value cannot be determined at the moment of its execution, the measures for complex inspection of the client shall be applied at the moment when the value of the operation or transaction is determined, if it is equal to or exceeds the BGN equivalent of EUR 2,000 or their equivalent in another currency, regardless of whether the operation or transaction was carried out through one operation or through several related operations.

The private enforcement agents apply the measures for complex inspection at each public sale carried out under the rules of the Civil Procedure Code, when the final price of the sold property is at a value equal to or exceeding the BGN equivalent of EUR 15,000 or their equivalent in another currency, regardless whether the payment was made through one or more related transactions.

The National Revenue Agency applies the rules for complex inspection in each case of public sale carried out under the rules of the Bulgarian Tax-Insurance Procedural Code when the final

price of the sold property is of a value equal to or exceeding the BGN equivalent of EUR 15,000 or their equivalent in another currency, regardless of whether the payment is made through one or more related operations the bodies of the National Revenue Agency apply the measures for complex verification.

The persons obliged to report must apply the measures for complex inspection in any case of suspicion of money laundering and/or the presence of funds of criminal origin, regardless of the value of the operation or transaction, the client's risk profile, the conditions for applying the measures for complex inspection or other exceptions provided for in this law or in the regulations for its implementation.

The measures for complex inspection of the clients under must be applied before the establishment of business relations, the opening of an account, the performance of a random operation or the conclusion of the random transaction, the performance of an operation or transaction, etc.

The persons obliged to report keep up-to-date the information collected through the application of the measures for complex inspection for their clients and for the operations and transactions performed by them, periodically reviewing and updating if necessary the maintained databases and client files, applying the measures for complex inspection.

The databases and the client files for the clients and the business relations with potentially higher risk shall be reviewed and updated on shorter periods.

If necessary, the topicality of the information is checked and additional actions for identification and verification of the identification are performed, when:

- an operation has been performed or a transaction has been concluded at a value different from the usual one for the client;

- there is a significant change in the way the account is used or in the way certain operations or transactions are performed;

- the information available for an existing client is insufficient for the purposes of the application of the measures for complex verification;

- a change has occurred in the circumstances.

In the cases where the person obliged to report cannot fulfill the requirements for complex inspection it must refuse the performance of the operation or transaction or the establishment of business relations, including the opening of an account.

If the business relationship has been already established and the person obliged to report cannot fulfil its obligations for complex inspection the relationship must be terminated.

These rules do not apply when it comes to the The Bulgarian National Bank in conducting transactions with foreign currencies, when their application contradicts the Bulgarian National Bank Act;

The private enforcement agents when their application contradicts the Civil Procedure Code and the Private Enforcement Agents Act;

the bodies of the National Revenue Agency, when their application contradicts the Tax-Insurance Procedure Code.

It is prohibited to open or maintain anonymous accounts or certificates of deposit, or accounts or certificates of deposit in an obviously fictitious name, as well as to rent or maintain anonymous safes or safes of obvious fictitious name.

Collection and preparation of documents and other information

Under the Bulgarian Anti-Money Laundering Act several types of information must be collected – customer identification, identification of the beneficial owner and identification of the origin of the funds.

- **Customer identification**

Customer identification and authentication are performed using documents, data or information from a reliable and independent source.

- **Identification of clients – natural persons**

The identification of the natural persons is carried out by presenting an official identity document and taking a copy of it. Regarding the natural persons the following data is being collected:

- the names;
- the date and place of birth;
- an official personal identification number or other unique element for establishing the identity, contained in an official identity document, the term of validity of which has not expired and on which there is a photo of the client;
- any citizenship that the person possesses;
- country of permanent residence and address (mailbox number is not sufficient).

Upon entering into business relations, data on the professional activity of the person and the purpose and nature of the person's participation in the business relations is collected by using

documents, data or information from a reliable and independent source, filling in a questionnaire or in another appropriate manner.

- **Identification of clients – legal entities**

The identification of legal entities is carried out by presenting an original or a notarized copy of an official extract from the respective register for their legal standing and a certified copy of the articles of association or other documents necessary for the collection of data mentioned below.

In the cases where a unique identification code issued in accordance with the regulations of the Bulgarian Commercial Register and the Register of Non-Profit Legal Entities Act has been presented and in the presence of an official public commercial or company register in a Member State in which the legal entity is registered, the identification of legal entities shall be carried out by reference in the commercial register or in the respective public register.

In the process of identifying the legal entities the persons obliged to report shall be obliged to establish its structure of ownership, management and control.

The following data is collected when it comes to legal entities:

- the name;
- the legal form;
- seat;
- the management address;
- the address for correspondence;
- the current activity carried out the legal entity and the purpose and nature of the business relations or of the random operation or transaction;
- the term of existence;
- the control bodies, the bodies of management and representation;
- the type and composition of the collective management body;
- the main place of commercial activity.

When a certain activity is subject to licensing, permission or registration, the clients, entering into business relations or performing transactions or operations in connection with this activity with or through a person obliged to report, shall present a certified copy of the respective license, permit or certificate for registration.

Identification of the beneficial owner

The identification of each natural person, who is the beneficial owner of a client - legal entity is carried out by collecting the following references and documents:

- extracts from the Bulgarian Commercial Register and the Register of Non-Profit Legal Entities, the Bulgarian Bulstat Register or the respective register in the country of origin in

cases of non-Bulgarian legal entities, where it is clearly stated which natural persons are the beneficial owner;

- certified copy of the articles of association, as well as other documents from which the beneficial owner and the nature and type of ownership or control are visible

- a declaration by the legal representative or by the proxy of the legal entity for the identification of the natural person who is the beneficial owner of a client - legal entity. This declaration can be used when the above-mentioned documents are insufficient or when they led to contradictory information.

Identification of the origin of the funds

According to the Bulgarian Anti-Money Laundering Measures Act in order to establish the origin of the funds at least two of the below-mentioned methods must be used:

- collection of information from the client about his main activity, including the actual and expected volume of the business relations and of the operations or transactions, which are expected to be performed within these relations, by filling in a questionnaire or in another appropriate way;

- collection of other information from official independent sources - data from publicly available registers and databases and others;

- use of information collected in connection with the fulfilment of the requirements of Anti-Money Laundering Measures Act or other acts, including the Currency Act, which can show a clear origin of the funds;

- use of information exchanged within the group to show a clear origin of the funds, where applicable;

- tracking of the cash flows within the established business relations with the client, whereby a clear origin of the funds is visible.

Information storage

The persons obliged to report must keep for a period of 5 years all documents, data and information, collected and prepared under the requirements of the Anti-Money Laundering Measures Act.

In the cases of establishing business relations with clients, as well as in the cases of entering into correspondent relations, the 5-year period starts running from the date of termination of the relationship.

In the cases of carrying out random operations or transactions the 5-yerar term starts running from the date of their execution.

It is possible upon a written instruction of the Director of the Financial Intelligence Directorate of the State Agency for National Security, for the term to be extended by no more than two years, when this is proportional and justified by the need to take appropriate actions for prevention or counteraction to money laundering or terrorist financing.

Assessment of the risk of money laundering and terrorist financing

According to the national anti-money laundering legislation of the Republic of Bulgaria there are two types of risk assessment – national and assessment carried out by the persons obliged to report.

National assessment of the risk

A national risk assessment of money laundering and terrorist financing is prepared and updated. every 2 years in order to identify, assess, understand and limit the risks of money laundering and terrorist financing for the purposes of the Anti-Money Laundering Measures Act and the Anti-Terrorist Financing Measures Act.

In preparing and updating the national risk assessment the competent authorities take into account and reflect the results of the supranational assessment of the risks of money laundering and terrorist financing prepared by the European Commission, which have an impact on the internal market and relate to cross-border activities. They also implement the recommendations of the European Commission to the Member States which are suitable for dealing with the identified risks.

The results of the national risk assessment are used for:

- improvement of the normative regulation for prevention and counteraction of money laundering and financing of terrorism, including by determination of all areas in which the persons obliged to report must apply more stringent measures and, where appropriate, an indication of the measures to be taken;

- identification of sectors or districts with a lower or higher degree of risk of money laundering and terrorist financing;

- distribution and targeting of the means and resources for counteraction to money laundering and terrorist financing;

- ensuring the preparation of appropriate rules for each sector or area in accordance with the risk of money laundering and terrorist financing;

- ensuring timely access of the persons obliged to report to the necessary information in order to facilitate the performance of their own risk assessments of money laundering and terrorist financing;

- preparation of a report on the institutional structure and basic procedures of the national system for prevention and prevention of money laundering and terrorist financing;

- preparation of a report on the national efforts and the human and financial resources engaged in the prevention and counteraction to money laundering and terrorist financing.

Assessment of the risk carried out by the persons obliged to report

In order to establish, understand and assess the risks of money laundering and terrorist financing, the persons obliged to report prepare their own risk assessments, taking into account the relevant risk factors, including those relating to customers, countries or geographical areas, the products and services offered, the operations and transactions performed or the delivery mechanisms.

When preparing and updating their risk assessment, the persons obliged to report must comply with the results of the national risk assessment, as well as with the results of the supranational risk assessment and the recommendations of the European Commission.

Disclosure of information regarding suspicious operations, transactions and clients

In case of doubt and/or finding out about money laundering and/or about the availability of funds of criminal origin, the persons obliged to report must notify immediately the Financial Intelligence Directorate of the State Agency "National Security" before the execution of the operation or transaction, delaying its implementation within the admissible term.

In the notification the maximum term in which the operation or transaction may be postponed must be indicated. Upon learning of money laundering or the of the existence of funds of criminal origin, the persons obliged to report must also notify the competent authorities in accordance with the Code of Criminal Procedure, with The Ministry of Interior Act and with The State Agency for National Security Act.

When the delay of the operation or transaction impossible or there is a probability that this will frustrate the actions for prosecution of the beneficiaries of the dubious transaction or operation, the person obliged to report must notify the Financial Intelligence Directorate of the State Agency "National Security" immediately after its implementation, indicating the reasons why the delay was impossible.

The notification to the Financial Intelligence Directorate of the State Agency for National Security may also be made by employees of the persons obliged to report, who are not responsible for the application of the measures against money laundering. The Directorate maintains the anonymity of these employees.

The Financial Intelligence Directorate of the State Agency for National Security provides to the person obliged to report information related to the notification made by him. The decision on the amount of information to be provided back for each specific notification case is taken by the director of the directorate.

When the notification is about suspicion of money laundering and/or suspicion of funds of criminal origin, the director of the Financial Intelligence Directorate of the State Agency for National Security may suspend with a written order a certain operation or transaction for within 5 working days from the day following the day of issuing the order, in order to perform an analysis, confirm the suspicion and disclose the results of the analysis to the competent authorities. When no attachment or foreclosure is imposed by the expiration of this term, the person obliged to report may perform the operation or transaction

After performing the analysis under within three working days, as of the day following the day of issuing the order, the Financial Intelligence Directorate of the State Agency for National Security must notify the prosecutor's office of the suspension of the operation or transaction, by providing the necessary information while maintaining the anonymity of the person, who has performed the notification.

The prosecutor may make a request to the relevant court for an attachment. The court should rule on the request no later than 24 hours after its receipt.

When during the investigation and analysis of the information obtained under the terms and conditions of this law, the suspicion of money laundering and/or related predicate offenses does not disappear, the Financial Intelligence Directorate of the State Agency for National Security shall disclose this information to the prosecutor's office of the respective security or public order service or of a competent specialized directorate of the State Agency "National Security" according to their competence.

Disclosure of other information

The persons obliged to report notify the Financial Intelligence Directorate of the State Agency for National Security for any payment in cash of over BGN 30,000 or their equivalent in foreign currency, made by or to their client within the established relations or in case of accidental transactions or operations. .

The Financial Intelligence Directorate of the State Agency for National Security keeps a register of the payments. The register may be used only for the purpose of combating money laundering and terrorist financing.

The Customs Agency provides the Financial Intelligence Directorate of the State Agency for National Security with information on trade credits for exports and imports, on financial leasing between local and foreign persons and on the transportation across the country of cash, precious metals and stones and articles with or from them, collected under the terms and conditions of the Currency Act.

Central Depository AD provides the Financial Intelligence Directorate of the State Agency for National Security with information on the issuance and disposal of dematerialized financial instruments according to certain criteria.

Control over the activity of the subjects obligated to report

The control over the application of the Anti-Money Laundering Act is exercised by the Chairman of the State Agency for National Security.

The control bodies are officials selected by the chairman of the State Agency "National Security". They are from the directorate "Financial intelligence" of the Agency.

The control bodies carry out on-site inspections of the persons obliged to report on the application of the measures for prevention of the use of the financial system for the purposes of money laundering, as well as in case of suspicion of money laundering.

In exercising this control the control bodies have the right to/of:

- free access to the official premises of the inspected person;
- request and collect documents, inquiries, extracts and other information in connection with the performance of the task assigned to them;
- request and collect copies of documents, certified by the inspected person or by a person authorized by him;
- require written and oral explanations for circumstances related to the subject of the inspection;
- to determine the term for submission of the documents, references, extracts, information and explanations.

For the purposes of the inspections experts may be used. Information, documents and other data necessary for the performance of these inspections may be required from third parties.

The inspected person shall be obliged to render assistance to the control bodies, as they:

- receive against signature the order for carrying out the inspection;
- provide a place for carrying out the inspection and appear upon request in the official premises of the State Agency "National Security";
- appoint its employee for contacts and rendering assistance to the control bodies;
- provide access to the office premises;
- provide within the term, determined by the control bodies, all documents, inquiries, extracts and other information, necessary for establishment of facts and circumstances, related to the scope and the subject of the inspection;

- upon request provide within the term determined by the control bodies, certified copies of documents, as the certification shall be done by affixing the inscription "True to the original", date and signature by a legal or authorized representative of the inspected person, as well as seal of the person obliged to report;

- upon request, give within the term, determined by the control bodies, written and oral explanations for circumstances, related to the subject of the inspection.

The control activity on the implementation of the measures for prevention of the use of the financial system for the purposes of money laundering is carried out by applying a risk-based approach, which consists of:

- identification of the relevant risk factors by collecting the necessary information, including in relation to risk clients, products and services;

- use of the collected information for assessment and understanding of the risk of money laundering and financing of terrorism, to which the persons obliged to report, as well as the measures taken by them to reduce and limit this risk;

- taking control measures proportionate to these risks and allocating resources in accordance with the risk assessment, including deciding on the scope, depth, duration and frequency of on-the-spot checks and the need for human resources. resources and expertise for carrying out the control activity;

- current monitoring and periodical review of the risk assessment and of the distribution of the resources for carrying out the control activity, including in case of occurrence of circumstances of essential importance or changes in the management and the activity of the persons under obliged to report, to ensure that risk assessment and resource allocation are up-to-date, applicable and relevant.

Exchange of information

The exchange of information regarding money laundering can be carried out on two levels – national and international.

- **Cooperation on a national level**

The supervisory authorities are obliged to provide information to the Financial Intelligence Directorate of the State Agency for National Security immediately if, in the course of their supervisory activities, they establish facts that may be related to money laundering.

The Financial Intelligence Directorate of the State Agency for National Security and the supervisory bodies may exchange information for the purposes of the statutory functions performed by them.

- **Cooperation on international level**

The Financial Intelligence Directorate of the State Agency for National Security may receive information on suspicion of money laundering through international exchange.

The Financial Intelligence Directorate of the State Agency for National Security must on its own initiative and upon request exchange information on suspicion of money laundering and related predicate offenses with the relevant international bodies, bodies of the European Union and bodies of other states on the basis of international agreements and/or under the conditions of reciprocity.

Requests from the Financial Intelligence Directorate of the State Agency for National Security to provide information to other financial intelligence units contain at least a description of the relevant facts, context, connection with the requested State, reasons for the request and the manner in which the requested information will be used.

For the purposes of the exchange, the Financial Intelligence Directorate of the State Agency for National Security provides the financial intelligence units of other countries with any type of information that it has or has direct or indirect access to, including natural and legal persons involved to the case.

The exchange of information cannot be refused due to the lack of information about the predicate offense.

The Financial Intelligence Directorate of the State Agency for National Security must immediately notify the financial intelligence unit of the respective Member State, when the received notification of money laundering or the presence of funds of criminal origin applies to that country.

Upon receipt of a motivated request of a unit for financial intelligence of another state and when there is a suspicion of money laundering, the director of the Financial Intelligence Directorate of the State Agency for National Security may suspend an operation or transaction.

The Financial Intelligence Directorate of the State Agency for National Security shall immediately notify the prosecutor's office of the suspension of the operation or transaction, providing the necessary information in compliance with the conditions and restrictions set by the financial intelligence unit of the respective country.

AML in Malta

The anti-money laundering measures in Malta aim to ensure the following - identification and verification of a customer and ultimate beneficial owner, record keeping, suspicious transaction reporting, training of employees.

1. Identification and verification of a customer

Regulation 7 of the PMLFTR sets out the CDD measures that are to be undertaken by subject persons in relation to their customers (and, where applicable, beneficial owners and agents) and the business relationships and occasional transactions that they seek to set up or carry out.

1.1. Identification of a natural person

Identification of a natural person takes place by obtaining a set of personal details. The standard set of personal details that is to be obtained for customers that are natural persons are the following:

- official full name;
- place and date of birth;
- permanent residential address;
- identity reference number, where available; and
- nationality.

Verification of the customer's identity takes place by making reference to documents, data or information obtained from a reliable and independent source such as:

- a government authority, department or agency;
- a regulated utility company; or
- a subject person carrying out relevant financial business in Malta or equivalent activities in a Member State of the EU52 or in a reputable jurisdiction.

1.2. Identification of companies

The subject person is required to first identify the company by gathering the following information:

- the company's official full name;
- the company's registration number;
- the company's date of incorporation or registration; and
- the company's registered address or principal place of business.

The subject person must verify all the information obtained on the company by referring to appropriate independent and reliable sources. It is up to the subject person to ascertain, following careful consideration of the risk posed by the customer, the appropriate sources. One or more of the following documents may be referred to by subject persons for verification purposes:

- the certificate of incorporation;
- a certificate of good standing (which is not older than three (3) months);
- a company registry search;
- the most recent version of the Memorandum and Articles of Association or other constitutive document;
- audited financial statements, annual returns, and/or tax returns for the previous or current year; and/or
- bank statements that are not older than six (6) months.

Once the verification is complete, the subject person must identify all the directors of the company. This information can be collected from the following sources:

- the list of directors contained in the most recent version of the Memorandum and Articles of Association;
- by performing a company registry search, provided that the officers of the company are listed therein;
- by referring to a good standing certificate or a certificate of incumbency, which is not more than three (3) months old; or
- by obtaining a copy of the directors' register of the company.

Subject persons are required to establish the company's ownership and control structure. While some structures are clear and easily understandable, other structures might be more complex and the use thereof without a legitimate commercial purpose should give rise to concern and possibly an increased risk of ML/FT. Subject persons should therefore undertake appropriate checks and gather information to be able to understand the ownership and control structure, and determine who is the customer's beneficial owner.

To comply with this obligation, subject persons must obtain from the customer and maintain on file or in electronic form an explanation of the company's ownership and control structure. In the case of multi-tier and complex structures, it would be also useful to maintain on file or in electronic form a chart showing the ownership structure to the extent that would be required to determine who the beneficial owner is.

2. Record keeping

Subject persons must have **procedures** in place and **apply** the same, **so as** to ensure that **the following records are maintained**:

- records of the actions taken to adopt and implement the risk-based approach, which are to include the following:
    - a copy of the BRA referred to in Section 3.3, changes thereto, as well as a record of any decision taken with respect to that assessment;
    - a copy of the subject person's most recent controls, policies, measures and procedures; and
    - a copy of each CRA carried out by the subject person and of any revision/s thereof.

- the CDD information and documents obtained for identification and verification of identity purposes. The records to be maintained are to include the following:
    - where subject persons view the original CDD documents, the original documents themselves (where it is possible to retain originals) or a true copy of these original documents, signed and dated by an officer of the subject person or a scanned copy retained by making use of the electronic system;
    - when subject persons receive a copy of the CDD documents, this copy should be maintained;
    - when subject persons use commercial electronic data providers, the results of the search should be maintained;

- when subject persons use video conferencing tools, identity verification software, or E-IDs to verify the identity of any individual, the records listed in those sub-sections should be retained;
- when the verification of the residential address of any individual is carried out by visiting that individual at the address indicated, a record of the visit should be maintained;
- when verification of the residential address of any individual is carried out by sending correspondence or codes via registered mail or other mail courier service, the records listed in that section should be retained;
- the documentation and other information obtained in fulfilment of the obligations should be retained; and
- any document obtained to ensure that the agent is duly authorised in writing to act on the customer's behalf should also be retained;

- records containing details relating to the business relationship that is formed and all transactions carried out in the course of a business relationship or an occasional transaction. These records are to include the following:
- information gathered on the purpose and intended nature of the business relationship and information gathered to establish the business and risk profile;
- files related to accounts held by the subject person, where applicable, and all business correspondence of the subject person exchanged in the course of a business relationship or in carrying out an occasional transaction;
- details on all transactions, whether international or domestic, carried out by the customers. The details should include:
  - the customer's and beneficiary's:
    - name,
    - address, or
    - other identifying information that is usually used by the subject person to identify parties to a transaction;
  - the nature and date of the transaction;
  - the type and amount of currency involved;
  - the type and identifying number of any account involved in the transaction;
  - the volume of funds flowing through the account; and
  - the origin of the funds, where necessary, and the form in which the funds were placed or withdrawn; and
- any supporting evidence and records necessary to reconstruct all transactions carried out or facilitated by that subject person in the course of a business relationship or any occasional transaction.

Such records should either consist of original documents or copies that are admissible in court proceedings.

Subject persons **should also retain the following records** required as evidence of compliance with the PMLFTR and for statistical purposes:

- internal reports made to the MLRO;

- a record of any written determinations made by the MLRO and the designated employee, including the reasons for not filing an STR with the FIAU;
- STRs made by the subject person to the FIAU and any follow-up submissions made in connection thereto;
- a record of AML/CFT training attended by sole practitioners/provided to employees;
- records of conduct certificates or other documentation obtained in carrying out employee screening, as referred to in Section 7.5;
- records of any outsourcing agreements entered into and other documentation that provides evidence of the subject person's adherence to its obligations under Chapter 6 of these Implementing Procedures, Part I;
- records of any reliance agreements entered into and of any related assessments undertaken on the other subject person or third party in terms of Section 4.10; and
- other important records, including:
  - any reports by the MLRO or by the officer entrusted with the monitoring function made to senior management made for the purposes of complying with the obligations under the PMLFTR, such as recommendations on internal procedures, correspondent banking relationships, PEPs, among others;
  - records of consideration of those reports made to senior management and of any action taken as a consequence thereof;
  - records of any internal audit reports or assessments dealing with AML/CFT issues; and
  - any other records that are necessary to demonstrate compliance with the obligations under the PMLA, the PMLFTR and any Implementing Procedures, Part I or any Sector Specific Implementing Procedures, Part II issued thereunder.

Subject persons must maintain the records for a period of **five (5) years**. The FIAU, relevant supervisory authorities or law enforcement agencies are entitled to demand that records, including personal data, **be retained for longer periods**, when this extension is considered necessary for the purposes of the prevention, detection, analysis and investigation of ML/FT activities by the FIAU, relevant supervisory authorities or law enforcement agencies.

3. Reporting on suspicious transactions

Regulation 15 of the PMLFTR requires a subject person to appoint one of its officers as the MLRO, whose core functions are to:

- receive reports from the subject person's employees of knowledge or suspicion of ML/FT, or that a person may have been, is or may be connected with ML/FT;
- consider these reports to determine whether knowledge or suspicion of ML/FT subsists or whether a person may have been, is or may be connected with ML/FT;
- report knowledge or suspicion of ML/FT or of a person's connection with ML/FT to the FIAU; and
- respond promptly to any request for information made by the FIAU.

The PMLFTR make reference to a general oversight function, as well as to the possible creation of a day-to-day monitoring function. ,

Day-to-Day Monitoring Function

In terms of Regulation 5(5)(c), a subject person has to appoint, where appropriate with regard to the nature and size of its business, an officer at management level whose duties are to include the monitoring of the day-to-day application of the measures, policies, controls and procedures adopted by the subject person to ensure compliance with its AML/CFT obligations.

In carrying out its business, a subject person may employ a considerable number of employees or structure its organisation in multiple units, offices or branches. Moreover, the business being carried out may itself involve a number of different activities. The same AML/CFT controls, policy measures and procedures would have to be applied and ensuring this is done in a uniform albeit flexible manner may prove impossible if there is no one officer charged with this responsibility.

When a subject person considers this function to be necessary, it is left to the subject person to determine whether this function is to be also carried out by the MLRO or whether it would prove to be more effective if it were entrusted to a separate officer. In the latter case, it would be especially important that communication between the two is as good as possible to ensure the effectiveness of the subject person's AML/CFT controls, policies, procedures and measures.
When the subject person opts to outsource its AML/CFT obligations in line with Chapter 6, the monitoring role would involve ensuring that the outsourced service provider is fulfilling its contractual obligations and carrying out the necessary controls, and to monitor the implementation of those AML/CFT obligations, if any, that have not been outsourced. In this scenario, the subject person has to decide, based on the volume of oversight work involved, whether a dedicated monitoring function is necessary or whether this role could be equally handled by the MLRO.

General Oversight Function

Given that the subject person is ultimately responsible for ensuring compliance with its AML/CFT obligations, the PMLFTR provide that the board of directors or administrators, or any other equivalent body responsible for the management of the subject person, may designate one of its members with responsibility to ensure that the subject person is fulfilling its AML/CFT obligations.

Internal reporting procedure

The procedures should clearly state that, when an employee has any such information, he/she is to report the matter to the MLRO without delay. Therefore, it is crucial that all employees are informed of the identity of the MLRO to whom the report has to be made, the procedure to follow and the information that has to be made available with the report.

Internal reports are to be submitted in writing, preferably using a standard template, together with all relevant information and documentation available to the employee to assist the MLRO in making a determination as to how best to proceed. The report should include details on the

customer who is the subject of concern and as full a statement as possible of the information giving rise to the knowledge or suspicion.

Reporting lines should be kept as short as possible, ideally allowing an employee to report directly to the MLRO to ensure speed, confidentiality and quick access to the MLRO. However, it is acknowledged that in larger organisations this may not always be possible and may even prove to be counter-productive. In these cases, it is acceptable for the internal reporting procedures to provide for intermediate filtering stages.

External reporting procedure

After considering the internal report and all the necessary documentation, when the MLRO or the designated employee determines that the subject person:

- knows;
- suspects; or
- has reasonable grounds to suspect that:
  - a transaction may be related to ML/FT; or
  - a person may have been, is or may be connected with ML/FT; or
  - ML/FT has been, is being or may be committed or attempted,

the MLRO must file an STR with the FIAU as set out hereunder.90 In so doing, the MLRO is not to disclose the name of the employee who made the internal report to the FIAU.

4. Training

It should be noted that awareness and training should be provided to employees and other company officials whose duties include the handling of either relevant financial business or relevant activity,102 irrespective of their level of seniority. This includes:
(a) directors;
(b) senior management;
(c) the MLRO and designated employee(s);
(d) compliance staff; and
(e) all members of staff involved in the activities of the subject person that fall within the definition of ‘relevant financial business’ and ‘relevant activity’.

Through training measures, the subject person should seek to ensure that relevant employees are knowledgeable of the subject person’s:
(a) CDD measures;
(b) record-keeping procedures;
(c) internal reporting procedures;
(d) the role of the MLRO in filing STRs with the FIAU (external reporting);
(e) risk management measures, including:

- customer acceptance policies;
- CRA procedures;
- internal controls;
- compliance management;
- communications;

- employee screening policies and procedures; and
- any other relevant policies and procedures concerning AML/CFT; and

(f) the ML/FT risks posed by the business and/or activities of the subject person (i.e., the outcomes of its BRA).

All employees should know who their MLRO, any designated employee(s) and the officer carrying out the monitoring function referred to in Section 5 are, as well as the functions and responsibilities of these key persons.

Employees should also be made aware of the following legislative instruments and other binding guidance:

(a) the provisions of the PMLA;
(b) the provisions of the PMLFTR;
(c) the provisions of the Criminal Code concerning the funding of terrorism;
(d) relevant data protection laws, rules and guidance;
(e) the FIAU Implementing Procedures, other guidance and/or interpretative notes issued by the FIAU; and
(f) the applicable offences and penalties resulting from breaches of all the above.

AML in the Netherlands

The legislation of the Kingdom of the Netherlands provides for several main anti-money laundering measures – identification and assessment of the risk of money laundering, conduction of client due diligence, reporting of unusual transactions, providing training to employees and adequate record-keeping.

1. Identification and assessment of risk

In order to prevent money laundering and terrorist financing, an institution conducts client investigations and reports unusual transactions. In doing so, an institution pays special attention to unusual transaction patterns and to transactions that by their nature involve a higher risk of money laundering or terrorist financing.

2. Record keeping

An institution that has conducted a client due diligence must record in an accessible manner the documents and data used for compliance with the provisions of the Dutch anti-money laundering legislation.

When it comes to natural persons, the documents and data include at least:

- the family name, given names, date of birth, address and place of residence, or the place of establishment of the client as well as of the person acting on behalf of that natural person, or a copy of the document containing a person-identifying number and on the basis of which the verification of identity has taken place;

- the nature, number and date and place of issue of the document verifying the identity;

When it comes to companies or other legal entities, the documents and data include at least:

- the legal form, the registered name, the trade name, the address with house number, the postcode, the place of establishment and the country of registered office;

- if the company or other legal entity is registered with the Chamber of Commerce, the registration number with the Chamber of Commerce and how the identity has been verified;

- of those who act for the company or legal entity at the institution: the family name, first names and date of birth.

When it comes to trusts or other legal arrangements, the documents and data include at least:

- the purpose and nature of the trust or other legal arrangement;

- the law governing the trust or other legal arrangement.

The institution keeps that data in an accessible manner for five years after the time of termination of the business relationship or for five years after the execution of the relevant transaction.

An institution that has reported an unusual transaction that has been carried out or is planned pursuant shall record the following information in a retrievable manner:

- all data that are necessary to be able to reconstruct the relevant transaction;

- a copy of the notification, as well as the information and data provided therewith;

- the notification from the Financial Intelligence Unit of receipt of this notification.

This information must be kept in an accessible manner for five years after the time of the notification or the time of receipt of the message from the Financial Intelligence Unit.

3. Training

The institution shall ensure that its employees, as well as the day-to-day policymakers, insofar as relevant for the performance of their duties and taking into account the risks, nature and size of the institution, are familiar with the provisions of this Act and periodically receive training that enable them to recognize an unusual transaction and to properly and fully conduct a customer due diligence.

4. Client due diligence

The institution conducts client due diligence to prevent money laundering and terrorist financing.

The Client due diligence enables the institution to:

- identify the client and verify his identity;
- identify the beneficial owner of the client and take reasonable steps to verify his identity, if the client is a legal person, take reasonable steps to gain an understanding of the ownership and control structure of the client, and if the beneficial owner is of the senior management, to take necessary reasonable steps to verify the identity of the natural person who is a member of the senior management, documenting the action taken and the difficulties encountered during the verification process;
- determine the purpose and intended nature of the business relationship;
- to continuously monitor the business relationship and the transactions made during the duration of that relationship to ensure that it reflects the client's knowledge of the institution and its risk profile, including an examination of the source of the resources used in the business relationship or transaction;
- to determine whether the natural person representing the client is authorized to do so and, if necessary, to identify the natural person and verify his identity;
- take reasonable measures to verify whether the client is acting for himself or for the benefit of a third party.

If a client acts as a trustee of a trust or for another legal construction, the customer due diligence also extends to the trust or legal construction. In that case, the client due diligence also enables the institution to determine whether the client is authorized to act as a trustee of a trust or for other legal arrangements.

If a client acts as a partner of a partnership, the customer due diligence. In that case, the client due diligence also enables the institution to determine whether the natural person representing the partners in the partnership is authorized to do so and, if necessary, to identify that person and verify his identity.

An institution conducts the client due diligence in the following cases:

- if it enters into a business relationship in or from the Netherlands;
- if it carries out an incidental transaction for the client in or from the Netherlands of at least EUR 15,000, or two or more transactions between which there is a connection with a combined value of at least EUR 15,000;
- if there are indications that the client is involved in money laundering or terrorist financing;
- if it doubts the correctness or completeness of previously obtained data from the client;

- if the risk of an existing client's involvement in money laundering or terrorist financing gives cause to do so;

- if there is an increased risk of money laundering or terrorist financing, having regard to the state in which a client resides or is established or has its seat;

- if it carries out an incidental transaction in or from the Netherlands for the benefit of the client or the trust, involving a transfer of funds as referred to in Article 3, ninth paragraph, of the Regulation on information to be attached to transfers of funds, amounting to at least EUR 1,000.

The institution attunes the client due diligence to the risk sensitivity to money laundering or terrorist financing of the type of customer, business relationship, product or transaction.

The institution takes reasonable steps to ensure that the information collected about individuals is kept up to date. In any case, the data must be updated if relevant circumstances regarding the client change, an institution is obliged under the Dutch anti-money laundering legislation to contact the client to evaluate information regarding the beneficial owner or the institution is obliged to do so under of Council Directive 2011/16 / EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/79 / EEC (OJ 2011, L 64).

5. Reporting of unusual transactions

The institution must immediately report an unusual transaction that has been made or is planned to take place after the unusual nature of the transaction has become known to the Financial Intelligence Unit.

When reporting the institution provides the following information:

- the identity of the client, the identity of the beneficial owners and, as far as possible, the identity of the person for whom the transaction is being executed;
- the nature and number of the identity document of the client and, as far as possible, of the other persons referred to under a;
- the nature, time and place of the transaction;
- the size and destination and origin of the funds, securities, precious metals or other assets involved in the transaction;
- the circumstances under which the transaction is classified as unusual;
- a description of the relevant items of great value in a transaction above € 15,000;
- additional information to be designated by order in council.

IV. PRACTICAL ASPECTS

Glossary Republic of Malta

MFSA Malta Financial Services Authority
AML Anti-Money Laundering
AMLD Anti-Money Laundering Directive
CDD Client Due Diligence
EDD Enhanced Due Diligence
CTF Combating Financing of Terrorism
ECHR European Court of Human Rights
SL Subsidiary Legislation
EU European Union
FATF Financial Action Task Force
STR Suspicious Transaction Report
FIAU Financial Intelligence Analysis Unit

KYC Know Your Customer
NRA National Risk Assessment
PEP Politically Exposed Person
SOE State Owned Entity
FT Financing of Terrorism
TM Transaction Monitoring
UBO Ultimate Beneficial Owner
MLRO Money Laundering Reporting Officer
PMLA Prevention of Money Laundering Act
IP Implementing Procedure
ML Money Laundering
PMLFTR Prevention of Money Laundering Funding of Terrorism Regulations

Glossary Kingdom Of Netherlands

AFM	Autoriteit Financiele Markten (Authority Financial Markets)
AML	Anti-Money Laundering
AMLD	Anti-Mponey Laundering Directive
BFT	Financial Supervision Office
CDD	Client Due Diligence
CTF	Combating Financing of Terrorism
DAC 6	Directive on Administrative Cooperation (The EU Council Directive 2011/16)
DCC	Dutch Criminal Code (Wetboek van Strafrecht)
DNB	Dutch National Bank (De Nederlandsche Bank)
DPPS	Dutch Public Prosecution Service
ECHR	European Court of Human Rights
EU	European Union
FATF	Financial Action Task Force
FIOD	Fiscal Intelligence and Investigation Service
FIU	Financial Intelligence Unit
ICBE	Institutions for Collective Investment in Securities
KYC	Know Your Client
NRA	National Risk Assessment
PEP	Politically Exposed Person
SOE	State Owned Entity
TF	Terrorist Financing
TM	Transaction Monitoring
UBO	Ultimate Beneficial Owner
UCITS	Undertakings for Collective Investment in Transferable Securities
UPC	Ultimate Parent Company
Wft	Financial Supervision Act
Wtt	Wet toezicht trustkantoren (Act on the supervision of trust offices)

Wwft Wet ter voorkoming van witwassen en terrorismefinanciering (Anti-money laundering and anti-terrorist financing act)

1. APPLICABLE AML LAWS AND REGULATIONS ON THE TERRITORY OF THE REPUBLIC OF BULGARIA, MALTA, KINGDOM OF NETHERLANDS

1.1 REPUBLIC OF BULGARIA

In the last few years, the Republic of Bulgaria has been working hard to create legislation related to measures against money laundering. There are two main legislative acts related to the fight against money laundering, but others contain additional rules. The acts are as follows:

Main Legislation in Republic of Bulgaria:

- Measures Against Money Laundering Act (MAMLA);
- Counter-Terrorism Act;
- Measures Against Financing of Terrorism Act.

Subsidiary Legislation in Republic Bulgaria:

- Rules on implementation of the Measures Against Money Laundering Act;
- Measures against financing of terrorism act.

Other relevant legislation connected with the measures against money laundering in Republic of Bulgaria:

- Credit Institutions Act;
- Currency Act;
- Payment Services and Payment Systems Act;
- Insurance Code;
- Markets in Financial Instruments Act;
- Act on The Operation of the Collective Investment Schemes and of Other Undertakings for Collective Investment;
- Code of Social Insurance;
- Act on Gambling.

1.2 REPUBLIC OF MALTA

• **Main Legislation:**

- Prevention of Money Laundering Act Cap. 373
- Proceeds of Crime Act Cap. 621

• **Subsidiary Legislation:**

- Prevention of Money Laundering and Funding of Terrorism Regulations, S.L. 373.01
- National Coordinating Committee on Combating Money Laundering and Funding of Terrorism Regulations, S.L. 373.02

- Centralised Bank Account Register Regulations, S.L. 373.03
- Use of Cash (Restriction) Regulations
- Companies Act (Register of Beneficial Owners) Regulations, S.L. 386.19
- Trusts and Trustees Act (Register of Beneficial Owners) Regulations, SL 331.10

• **FIAU Implementing Procedures**

- Implementing Procedures – Part 1
- Implementing Procedures (Banking Sector) – Part 2
- Implementing Procedures – Part 2 Land Based Casinos
- Implementing Procedures – Part 2 Remote Gaming Sector
- Implementing Procedures – Part 2 Virtual Financial Assets Sector
- Implementing Procedures – Part 2 Company Service Providers

• Other relevant legislation

- (Maltese) Criminal Code Cap. 9
- Dangerous Drugs Ordinance – Ordinance – Cap. 101 of the Laws of Malta
- Income Tax Act – Cap. 123 of the Laws of Malta
- National Interest (Enabling Powers) Act – Chapter 365 of the Laws of Malta

- **EU and International level**:

- DIRECTIVE (EU) 2015/849 Of the European Parliament and of the Council of 20 May 2015
- DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018
- REGULATION (EU) 2015/847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2015
- Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating ML by criminal law
- COMMISSION DELEGATED REGULATION (EU) 2016/1675 of 14 July 2016
- COMMISSION DELEGATED REGULATION (EU) 2018/1108 of 7 May 2018
- COMMISSION DELEGATED REGULATION (EU) 2019/758 of 31 January 2019
-

1 EU measures: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money laundering-and-counter-terrorist-financing_en#latest

Foreign Acts and soft law:

- FATF Recommendations
- Results ML/TF National Risk Assessment

1.3 KINGDOM OF THE NETHERLANDS

Main Legislation:

Anti-Money Laundering and Anti-Terrorist Financing Act Wet ter voorkoming van witwassen en terrorismefinanciering ("**Wwft**") 2018 - transposing the EU 4th AML Directive. This is the primary act for prevention of money laundering and terrorist financing in the Netherlands;

- Implementation Regulation AMLA
- Act on the Supervision of Trust Offices (Wtt) 2018 – primary aiming at improving the integrity of trust offices (corporate service providers)
- Act of Financial Supervision (Wft)
- Dutch Criminal Code (Wetboek van Strafrecht)
- Taxation Act
- The Integrity Promotion Act for Public Administration (Bibob Act)
- Sanctions Act 1977
- Trade Register Act 2007, implementing partially the 5th AML Directive and introducing the obligation of UBO registration

EU and International level:

- Fifth EU Anti-Money Laundering Directive 2018/843 (AMLD5) and fourth AML Directive
- Directive 2006/70/EU (PEP Directive)
- FATF Recommendations 2012 (amended in 2020)

Foreign Acts and soft law:

- Good Practices Transaction Monitoring – DNB 2017
- DNB Guidance on AML and CTF and SA 2019
- Transaction Monitoring Guidelines Holland Quaestor
- Guidance Wtt and Wwft
- National Risk Assessment AML 2017
- Explanatory memorandum on the Wwft

2. OBLIGED ENTITIES UNDER THE AML LEGISLATION IN BULGARIA, MALTA, THE KINGDOM OF THE NETHERLANDS

2.1.REPUBLIC OF BULGARIA

The Measures Against Money Laundering Act outlines the measures that must be taken to prevent money laundering and specifies the entities that must implement these measures.

According to Art. 4 of MAMLA, the obliged entities are the following:

1. **The Bulgarian National Bank and the credit institutions,** which perform activity on the territory of the Republic of Bulgaria in the meaning of the Credit Institutions Act;

2. **the other providers of payment services** in the meaning of the Payment Services Act and the Payment Systems and their Representatives;

3. t**he financial institutions in the meaning of the Credit Institutions Act;**

4. **the currency exchange desks;**

5. **insurers, reinsurers and insurance firms with central offices in the Republic of Bulgaria**,

6. **the post operators, licensed to carry out post money transfers under the Postal Services Act**;

7. **investment companies that have been licensed under the terms and procedures of the Markets in Financial Instruments Act;**

8. **collective investment schemes and other undertakings for collective investment** that have been licensed and obtained permit under the terms and conditions of the Act on the Operation of the Collective Investment Schemes and of Other Undertakings for Collective Investment;

9. **the managing companies and persons, managing alternative investment funds**

10. **that have been licensed under the terms and conditions of the Act on the Operation of the Collective Investment Schemes and of Other Undertakings for Collective Investment;**

11. **pension security companie**s with the exception of their activity on the management of funds for additional compulsory pension security;

12. **the registered auditors;**

13. **persons, who upon profession provide accounting services and/or consultations in the area of taxation;**

14. **persons, who upon profession provide accounting services and/or consultations in the area of taxation,** as well as persons, who, as a principal business or professional activity, provide, directly or indirectly, through related persons, assistance in any form or advice on tax matters;

15. **persons, who upon profession carry out legal consultations, where:**

a) they assist or participate in planning or fulfillment of an operation, transaction or other legal or factual action of their client about:

- a purchase - sale of real estate or transfer of undertaking to a trader;
- management of funds, financial instruments or other assets;
- opening, managing or disposition with a bank account, with deposit account to an account for financial instruments;

- procurement of funds for establishing a legal person or other legal formation, increasing the capital of a trade company, provision of loan or any other form of procurement of funds for realization of the activity of a legal person or other legal formation;
- establishing, registration, organization of the activity or management of trust ownership, trader or other legal person or other legal formation;
- trust management of property, including trusts, custodian funds and other similar foreign legal formations, established and existing pursuant to the law of jurisdictions, admitting such forms of trust ownership;

b) they act at the expense of and/or on behalf of own client in any financial operation;
c) they act at the expense of and/or on behalf of own client in any transaction with real estate;
d) they provide management address and correspondence address, office and/or other similar services for the purposed of registration and/or functioning of a legal person or other legal formation;

16. **the persons who upon profession provide:**

a) management address, correspondence address, office and/or other similar services for the purposes of registration and/or functioning of a legal person or other legal formation;

b) services of establishment, registration, organization of the activity and/or management of a trader or other legal person or other legal formation;

c) services of trust management of property or of a person under latter “b”. including:

- fulfillment of the position or organization of execution by another person at the position of director, secretary, partner or other similar position in a legal person or other legal formation;

- execution of the position or organization of execution by another person of the position trust owner – in the cases of trusts, custodian funds and other similar foreign legal formations, established and existing according to the law of jurisdictions, admitting such forms of trusted ownership;

- execution of the position or organization of execution by another person the position of nominal shareholder in a third foreign legal person or another legal formation, other than a company, whose assets are traded on a regulated market, to which the requirements of information in compliance with the EU law or of equivalent international standards are applied;

17. **the private enforcement agents and assistant private enforcement agents;**

18. **persons, who execute upon profession intermediation in transactions with real estates, including with respect to real estate leasing transactions, where the monthly rent amounts to, or exceeds EUR 10,000 or their equivalent in another currency**;

19. **wholesale traders;**

20. **traders of weapons, petrol and petrol products;**

21. **organizations of gambling games;**

22. **organizations on privatization;**

23. **persons, organizing awarding of public procurement;**

24. **ministers and municipality mayors while signing concession contracts;**

25. **legal persons, at which there are mutual assistance funds;**

26. **persons, who provide money loans against betting on items;**

27. **professional unions and branch organizations;**

28. **non-profitable legal persons;**

29. **professional sport clubs;**

30. **market operators and/or regulated markets** that have been licensed under the terms and procedures of the Markets in Financial Instruments Act;

31. **the central securities depositories;**

32. **political parties;**

33. **the bodies of the National Revenue Agency;**

34. **customs bodies;**

35. **the executive director of the Environment Executive Agency;**

36. **persons, who, by occupation, trade or act as intermediaries in the trade in works of art,** including when carried out by art galleries and auction houses, when the value of the transaction or related transactions amounts to**, or exceeds EUR 10,000, or their equivalent in another currency;**

37. **persons, who, by occupation, store, trade or act as intermediaries in the trade in works of art**, when this is done in free zones and when the value of the transaction or related transactions amounts to, **or exceeds EUR 10,000 or their equivalent in another currency;**

38. the persons, who, by occupation provide services for the exchange between virtual currencies and recognized currencies, without gold coverage;

39. **Portfolio providers, offering custody services.**

2.2.REPUBLIC OF MALTA

Article 2.1 of the Implementing Procedures outlines the 'Subject Persons' who are subject to reporting obligations, on the basis that they undertake 'relevant activities' or 'relevant financial business'. The definition of 'Subject Persons' includes the following:

(a) **auditors, external accountants and tax advisors**, including when acting as provided for in paragraph (c);

(b) **real estate agents;**

(c) **notaries and other independent legal professionals** when they participate, whether by acting on behalf of and for their client in any financial or real estate transaction or by assisting in the planning or carrying out of transactions for their clients concerning the: (i) buying and selling of real property or business entities; (ii) managing of client money, securities or other assets, unless the activity is undertaken under a licence issued under the provisions of the

Investment Services Act22; (iii) opening or management of bank, savings or securities accounts; (iv) organization of contributions necessary for the creation, operation or management of companies; (v) creation, operation or management of companies, trusts, foundations or similar structures, or when acting as a trust or company service provider;

(d) **trust and company service providers;**

(e) **nominee companies holding a warrant under the Malta Financial Services Authority** Act23 and acting in relation to dissolved companies registered under the said Act;

(f) **casino licensees;**

(g) **gaming licensees**; and

(h) **any natural or legal person trading in goods, but only where a transaction involves payment in cash** in an amount equal to ten thousand euro (€10,000) or more whether the transaction is carried out in a single operation or in several operations which appear to be linked.

On the other hand individuals/entities undertaking 'Relevant financial business' is defined in the PMLFTR are also subject to reporting obligations, these including:

(a) **any business of banking carried on by a person or institution** who is for the time being licensed, or required to be licensed, under the provisions of the Banking Act24;
(b) any activity of a financial institution carried on by a person or institution who is for the time being licensed, or required to be licensed, under the provisions of the Financial Institutions Act;

(c) **any long-term insurance business other than business of reinsurance** carried on by a person or institution who is for the time being authorised, or required to be authorised, under the provisions of the Insurance Business Act25;

(d) **any insurance intermediary activities carried out by an insurance intermediary or by a tied insurance intermediary** related to long-term insurance business which person or institution is enrolled or required to be enrolled under the provisions of the Insurance Distribution Act26, other than a natural person who is registered or enrolled and acts on behalf of a tied insurance intermediary or a person or institution enrolled as a tied insurance intermediary that does not collect premiums, or other amounts intended for the policyholder or the beneficiary;

(e) **any long term insurance business other than business of reinsurance** carried on by a person in accordance with the Insurance Business (Captive Insurance Undertakings and Captive Reinsurance Undertakings) Regulations27, by a cell company in accordance with the

22 Chapter 370 Laws of Mala
23 Chapter 330 Laws of Malta
24 Chapter 331 Laws of Malta
25 Chapter 403 Laws of Malta
26 Chapter 487 Laws of Mala
27 Subsidiary Legislation 403.11 Laws of Malta

provisions of the Companies Act (Cell Companies Carrying on Business of Insurance) Regulations28 or by an incorporated cell company and an incorporated cell in accordance with the provisions of the Companies Act (Incorporated Cell Companies Carrying on Business of Insurance) Regulations;

(f) **investment services carried on by a person or institution** licensed or required to be licensed under the provisions of the Investment Services Act;

(g) **administration services to collective investment schemes** carried on by a person or institution recognised or required to be recognised under the provisions of the Investment Services Act other than administration services provided by recognised incorporated cell companies in accordance with the Companies Act (Recognised Incorporated Cell Companies) Regulations;

(h) **a collective investment scheme marketing its units or shares**, licensed, recognised or notified, or required to be licensed, recognised or notified, under the provisions of the Investment Services Act;

(i) **any activity other than that of a retirement scheme or a retirement fund**, carried on in relation to a retirement scheme, by a person or institution licensed or required to be licensed under the provisions of the Retirement Pensions Act29 and for the purpose of this paragraph, ‘’retirement scheme’’ and ‘’retirement fund’’ shall have the same meaning as is assigned to them in the Retirement Pension Act;

(j) any activity of a regulated market and that of a central securities depository authorised or required to be authorised under the provisions of the Financial Markets Act30;

(k) **safe custody services provided by any person or institution** not covered under paragraph (a) or (f);

(l) **any activity of a VFA agent carried out by a person or institution** registered or required to be registered under the provisions of the Virtual Financial Assets Act31;

(m)**VFA services carried out by a person or institution** licensed or required to be licensed under the provisions of the Virtual Financial Assets Act;

(n) **the issue of virtual financial assets for offer to the public in or from Malta** in terms of the Virtual Financial Assets Act; and

(o) **any activity under paragraphs (a) to (k) carried out by branches** established in Malta and whose head offices are situated outside Malta.

2.3.THE KINGDOM OF THE NETHERLANDS

The defines under the term 'entity' to whom the Act applies. The term entity includes both natural and legal persons.

The Wwft applies to the following institutions (Article 1a Wwft):

- **Accountants**
- **Lawyers**
- **Banks**
- **Tax advisors**
- **Investment institutions**
- **Investment firms**
- **Life insurance brokers**
- **Payment service agents**
- **Payment service implementers acting for a payment service provider with a license from another EU member state**
- **Payment service providers**
- **Natural or Legal persons that put their address at another's disposal**
- **Electronic money institutions**
- **Traders / sellers of goods**
- **Institutions for Collective Investment in Securities (ICBE)**
- **Institutions, not being banks, that carry out banking activities**
- **Civil-law notaries**
- **Pawn shops**
- **Casinos**
- **Valuers**
- **Trust offices**
- **Safe custody services**
- **Money-exchange institutions**

3. MAIN MEASURES AND OBLIGATIONS FOR THE OBLIGED ENTITIES UNDER THE AML LEGISLATIONS IN BULGARIA, MALTA, THE KINGDOM OF THE NETHERLANDS (COMPLIANCE REQUIREMENTS);

3.1.REPUBLIC OF BULGARIA

The MAMLA clearly states the measures for the prevention of using the financial system for money laundering. These are:

1. a complex check of the clients;
2. collecting and drawing up documents and other information under the conditions and procedure of this act;
3. keeping of the collected and drawn up for the purposes of this act documents, data and information;
4. risk assessment from money laundering and financing terrorism;
5. disclosure of information about suspicious operations, transactions and clients;
6. disclosure of other information for the purposes of MAMLA;
7. control over the activity of the obliged subjects under MAMLA;
8. exchange of information and cooperation at a national level, as well as an exchange of information and cooperation between Financial Intelligence of Directorate of the National Security State Agency, the units for financial intelligence of other state and jurisdictions as well as with the competent bodies and organizations of other states in the relevant area.

In order to identify, understand and assess the risks of money laundering and terrorist financing, obligated entities shall make their own risk assessments, taking into account relevant risk factors, including those relating to customers, countries or geographical areas, products and services offered, the operations and transactions performed or the delivery mechanisms.

On the other hand, in connection with the obligations specified in the MAMLA, the obliged entities shall also adopt internal rules for control and prevention of money laundering and financing of terrorism.

3.2.REPUBLIC OF MALTA

Objective of the PMLA

The objective of the PMLA is to maintain the integrity of Malta's financial system by combating the fight against money laundering and funding of terrorism. The PMLA establishes the foundations for the legal framework by introducing basic legal definitions, laying down the procedures for the investigation and prosecution of money laundering offences, and establishing Malta's Financial Intelligence Unit and AML/CFT regulatory and supervisory authority.

Risk-oriented approach

This involves the risk, obliged entities are exposed to prior to adopting and applying any measures, policies, controls and procedures to mitigate the same. In order for obliged entities to assess risk, it is first necessary to identity and understand how risk can manifest by analysing the following variables that either on their own or in conjugation with each other may increase or decrease risk posed to obliged entities:

1. Customer Risk
2. Geographical Risk
3. Product, Service and Transaction Risk
4. Delivery Channels Risk
5. Additional Risk Factors – e.g. exposure risk

The risk factors obliged entities may be exposed to, will vary depending on the nature and size of the business, understood as being both its structures and systems, as well as its actual activities.

The risk-oriented approach hinges on two main aspects: an understanding of the risks one is facing and, based on this understanding, the variation of one's controls, policies, measures and procedures to achieve the strongest mitigating effect possible. This calls not only for an understanding and assessment of risk that one's business is in general exposed to, but also for a more specific assessment of the risk to which obliged entities will be exposing themselves to when establishing individual business relationships or carrying out a given occasional transaction.

Customer screening

The implementation of a sound customer screening programme is key for obliged entities to determine whether a prospective customer falls within their risk appetite. Through customer screening, obliged entities collate information about their customers to assess the extent of any risk they pose to them by carrying out the following steps:

- To determine who the customer and, where applicable, the beneficial owner is;
- To verify whether that person is the person he/she purports to be;
- To determine whether a person is acting on his/her own behalf or on behalf of another person (e.g., an agent, signatory, attorney, etc.);

- To establish the purpose and intended nature of the business relationship, and the customer's business and risk profile; and
- In the case of a business relationship, monitor that relationship on an ongoing basis.

Identification of the customer and the verification of the customer's identity takes place by making reference to documents, data or information obtained from a reliable and independent source. Through the identification and verification of identity procedures carried out, obliged entities have to be satisfied that he/she knows and has verified that the customer exists, and that the customer is who he/she purports to be.

The standard set of personal details that is to be obtained for customers that are natural persons are the following:

1. official full name;
2. place and date of birth;
3. permanent residential address;
4. identity reference number, where available; and
5. nationality

The implementation of a sound customer screening programme is key for all obliged entities to safeguard their services and products from being misused and ending up as conduits for proceeds of crime or being used for ML/FT purposes.

The implementation of CDD measures enables subject persons to assist the FIAU and Maltese law enforcement authorities to carry out their responsibilities of analysing and investigating cases of ML/FT in an effective manner.

Transaction Monitoring and reporting of unusual transactions

Transaction monitoring is important for obliged entities to identify behaviour or transactions that diverge from the usual pattern of transactions, identify suspicious activity in relation to which an STR is to be filed with the FIAU and to determine whether the initial risk assessment requires updating, and whether, in view of the updated risk assessment or other considerations, the business relationship remains within the subject person's risk appetite.

Periodic training of employees

Regular periodic training to all employees and other company officials whose duties include the handling of either relevant financial business or relevant activity, irrespective of their level of seniority, to ensure that they are fully alert to the very real risks of money laundering and the funding of terrorism, in the identification of unusual transactions, and riskier situations that may turn out to be suspicious, is critical to the success and effectiveness of a subject person's efforts at combatting ML/FT32.

Training needs to be well thought out and planned, targeted but also proportionate, depending on the nature of the obliged entities activities, the risks it is exposed to, as well as the size of the obliged entities business or operation.

32 Regulations 5(5)(b) and (e) PMLFTR

Record-keeping

Obliged entities must, from a purely ML/FT viewpoint, retain all records for a period of five (5) years33 after the termination date of servicing a client of any business relationship / occasional transaction carried out.

However, the FIAU, relevant supervisory authorities or law enforcement agencies are entitled to demand that records, including personal data, be retained for longer periods, when this extension is considered necessary for the purposes of the prevention, detection, analysis and investigation of ML/FT activities by the FIAU.

3.3.KINGDOM OF THE NETHERLANDS

Objective of the Wwft

The objective of the Wwft is to maintain the integrity of the financial system. Public confidence in this system is severely damaged if parts of the system are used to launder the proceeds of crime and to finance terrorism. As a result of the Wwft, not only the information position of the investigative services and the judiciary is strengthened, but also of the reporting entities.

Risk-oriented approach

Taking measures to identify and assess its risks of money laundering and terrorist financing, including the recording of the results of such assessments. In addition, the obligation exists to have policies and procedures in place to mitigate and effectively manage the risks of money laundering and terrorist financing and the risks identified in the national risk assessment (Articles 1f – 2d Wwft). The Wwft has a risk-oriented approach. This means that the entities themselves have to assess the risks certain customers or products entail. The Act offers the entities the possibility to adjust their efforts to these risks. This approach has been incorporated in the entity's own compliance regulations and fits within their responsibilities and the duty of due care to which they are subject. The internal regulations are custom-made and become more stringent as the estimated risk increases. In addition, the Wwft does not prescribe as mandatory how an entity must achieve a result; it only describes the required result.

Customer screening

Conducting a thorough – standard, simplified or strengthened customer due diligence (CDD) prior to entering into a business relationship or conducting (incidental) transactions (Articles 3-11 Wwft). A customer's identity must be verified and recorded before the transaction takes place. Identification of customers is not only relevant at first contact, but also applies to long-lasting relations and specific incidental transactions. The entity requests each customer to personally present a valid ID document. Once the identity of a customer has been established, and he or she returns regularly, the entity does not have to ask for ID on every visit.

Transaction Monitoring and reporting of unusual transactions

Pursuant to the Wwft, FIU-the Netherlands is the organization to which entities with an obligation to report should report unusual transactions. With its analysis of reported unusual transactions, FIU-the Netherlands uncovers money flows that can be linked to money laundering, the financing of terrorism, or underlying crimes. After the transactions have been declared suspicious by the head of the FIU-the Netherlands, they are put at the disposal of various law enforcement and investigative services (Articles 12-23a Wwft).

Periodic training of employees

Providing periodic training to employees in order for them to be able to recognize unusual transactions and conduct a proper and comprehensive CDD (Article 35 Wwft).

Record-keeping

Adequate record-keeping of risk assessment/CDD and reporting of unusual transactions and providing these results to regulators upon request (Articles 33-34 Wwft).

4. REGULATORY INSTITUTIONS FOR AML COMPLIANCE IN BULGARIA, MALTA, THE KINGDOM OF THE NETHERLANDS AND METHODS OF ACTION;

4.1.Bulgaria

In chapter nine of MAMLA are specified the institutions that exercise control over the obliged entities. One of the regulatory institutions mentioned in the act is National Security State Agency (NSSA). NSSA exercises control over the implementation of MAMLA. The chairman of MAMLA determines control bodies and gives them instructions for carrying out the checks. The checks shall be performed on the basis of a written order of the chairman of the NSSA or of an official, authorized by him.

Other institution is the Bulgarian National Bank (BNB). The BNB exercises control over:]

1. the persons, licensed by it credit institutions, including branches of third-country credit institutions, as well as with respect to branches of credit institutions, established in the Republic of Bulgaria, licensed in other Member States;
2. licensed by its other payment service providers within the meaning of the Payment Services and Payment Systems Act and their representatives.

Next, control is exercised also by the Financial Supervision Commission (FSC) over:

1. insurers and insurance firms;
2. investment firms;
3. collective investment schemes and other undertakings for collective investment;
4. the managing companies and persons, managing alternative investment funds;
5. pension security companies.

Control exercises and the National Revenue Agency over the following entities: the organizers of gambling games, who have received a license for organizing gambling games on the territory of the Republic of Bulgaria.

4.2. Malta;

Maltese AML regulations have been created to be compatible with FATF and European Union regulations.

The Malta Financial Services Authority (MFSA) is a public institution that regulates and supervises financial institutions. With the AML / CFT Co-ordination Committee it is aimed to prevent money laundering and terrorist financing. The Malta Financial Services Authority (MFSA) publishes AML regulations and guidelines that support Maltese legislation. MFSA and FIAU jointly conduct AML / CFT audit in Malta.

The Financial Intelligence Analysis Unit (FIAU) is a national Maltese institution responsible for preventing money laundering and financing terrorism. The Financial Intelligence Analysis Unit is responsible for collecting and investigating financial crime information.

4.3.The Kingdom of the Netherlands.

The Dutch Ministry of Finance has appointed a number of supervisory authorities to ensure that reporting entities comply properly with the obligation to report. FIU-the Netherlands works together with the supervisory authorities to provide information to various groups of entities.

One important component of the monitoring role is checking that entities have a suitable administrative organization in place, including internal auditing procedures. The entity's administration must be of a sufficient standard to enable the entity to carry out customer research and to ensure that staff recognize unusual transactions and report them to FIU-the Netherlands. In addition, the supervisory authorities ensure that the entities actively carry out customer research and do indeed report any unusual transactions.

The supervisory authorities for the Wwft are:

- De Nederlandsche Bank (DNB): The DNB is responsible for monitoring compliance with the Wwft by banks, credit institutions, money exchange institutions, electronic money institutions, payment institutions, life insurers, trust offices, casinos, and safe custody services.

- The Netherlands Authority for the Financial Markets (AFM): The AFM is responsible for monitoring compliance with the Wwft by investment companies, banks and financial service-providers to the extent that they act as life-insurance brokers, and Undertakings for Collective Investment in Transferable Securities (UCITS).

- Financial Supervision Office (BFT): The BFT is responsible for monitoring compliance with the Wwft by accountants, tax consultants, and civil-law notaries.

- The Dutch Tax Authority and Wwft Supervision Office: monitors agents or brokers in high-value goods, valuers, dealers or traders in goods, pawnbrokers, and natural or legal persons that put their address at the disposal of another.

- The dean of the Bar Association in the legal district is responsible for the supervision of lawyers (attorneys-at-law).

- The Dutch Gaming Authority (KSA): regulator for gaming casinos.

- The Dutch police and Fiscal Intelligence and Investigation Service (FIOD), responsible for investigating money laundering.

The WWFT provides for the exchange of information between the supervisory authorities and FIU-Netherlands with regard to reporting behaviour of the entities with an obligation to report. Such information is frequently exchanged.

5. HIGHLIGHTS (MAIN POINTS) OF THE NATIONAL RISK ASSESSMENT IN BULGARIA, MALTA, THE KINGDOM OF THE NETHERLANDS;

5.1.Bulgaria;

Money laundering and financing terrorism is a topic of discussion not only in the European Union and his institutions but also in the Member States. The European Union adopts legal acts for prevention of money laundering and terrorist financing permanently.

One of the measures for preventing money laundering and financing terrorism is adopting a supranational risk assessment. The European Commission carries out risk assessments in order to identify and respond to risks affecting the EU internal market. It promotes the adoption of global solutions to respond to these threats at international level.

On 26 June 2017 the Commission published its first Supranational Risk Assessment Report as required by the 4th anti-money laundering Directive. The Commission assessed the vulnerability of financial products and services to risks of money laundering and terrorist financing. This risk analysis is conceived as a key tool to identify, analyze and address money laundering and terrorist financing risks in the EU. It aims at providing a comprehensive mapping of risks on all relevant areas, as well as recommendations to Member States, European Supervisory Authorities and obliged entities to mitigate these risks. This risk analysis support Member States and obliged entities when carrying out their respective risk assessments. On 24 July 2019, the Commission published its second supranational risk assessment report.

Based on this Supranational risk assessment, the Member States are obligated to adopt a national risk assessment after considering and reflecting the results of the Supranational Risk Assessment of money laundering and terrorist financing prepared by the European Commission, which have an impact on the internal market and relate to cross-border activities, following the recommendations of the European Commission.

NATIONAL RISK ASSESSMENT OF REPUBLIC BULGARIA

Under Art. 95 of Measures Against Money Laundering Law (MAMLL), there is an obligation for carrying out a National Risk Assessment (NRA) for establishing, assessment, understanding and limitation of the risk from money laundering and financing terrorism. The NRA shall be updated every two years and is accepted in fulfillment of an obligation arising from the FATF Recommendations, as well as from the requirements of the preventive legislation against money laundering and the financing of terrorism of the European Union

(EU). The last one was published in 2020 and it is expected the next one to be published in 2022.

The NRA which was published in 2020 is the first holistic assessment that analyzes the internal and external risks of money laundering and financing terrorism. The main purpose of the NRA is to contribute of taking appropriate risk measures against money laundering and financing terrorism. This risk assessment is a step for identification and assessment of threats and vulnerabilities to money laundering and financing terrorism for Bulgaria. The NRA is a result of consultations between different enforcement authorities, national security authorities, supervisory authorities and other public authorities and private sector and reflects the information provided by them. Sources of information include public national and international reports in the relevant filets, including those published by Europol, FATF, the Council of Europe's Monival Committee and the Supranational risk assessment of the risk of money laundering and financing terrorism of the European commission.

The NRA is based on detailed analyze of the risks from money laundering and financing terrorism on the following components:

- analysis of the threats arising from predicate criminal activity, which is a major source of criminal means;
- analysis of the subjects, which are engaged in money laundering activities;
- analysis of the economic sectors related to money laundering;
- analysis of financial sector and the sector of non-financial businesses and professions used for money laundering and terrorist financing purposes;
- cross-border characteristics of money laundering;
- analysis the risks of financing terrorism.

THE NRA CONCLUDES THE MAIN RISK EVENTS, SUCH AS:

- Money laundering from wide range of predicate offences, carried out abroad or on the territory of the country, related to organized crime through the use of formal financial system and the widespread use of cash.
- Money laundering, acquired from corruption by complex schemes for money laundering on the territory of the country or abroad with the help of "professional money launderers" and the subsequent integration of funds in financial instruments abroad and in legal entities and real estate in the country;
- Money laundering from tax crimes through the use of strawman, local and foreign legal entities in complex schemes for stratification and with the help of "professional washers";
- Integration by local and foreign persons of significant amounts of "laundered funds" in the sector of construction and real estate investments in the context of a significant share of the gray economy;
- Money laundering of carried out abroad predicate crimes through the use of non-bank investment intermediaries in Bulgaria, as well as cases of unregulated trading in financial instruments;

- Laundering of funds, acquired from tax crimes in the field of trade in food and fuel by using hollow companies and nominal owners, assisted by the corruption environment and the "gray economy";
- Laundering of funds, obtained from computer fraud and “social engineering” fraud, committed by small or medium-sized organized criminal groups, which use the territory of country to stratify the funds;
- The possible involvement of professionals and obligated entities under the MAMLL, facilitated by vulnerabilities related to the rules for admission to the market and the selection of their employees, as a major risk that supports the functioning of organized crime and contributes to the level of most of the above risks.

The NRA also concludes high-risk events from financing terrorism, such as:

- The use of services for available money transfers for the transfer of funds potentially related to financing terrorism for which also contributes to migrant communities, further influenced to a large extent by the cash and gray economy;
- Diversion of funds which is a potential risk, intended for the activity of non-profit legal entities or for religious activities in Bulgaria for financing terrorism.

THREATS ACCORDING TO THE NRA:

The NRA describes the threats which are related with money laundering. They are divided into two types of threats.

The first is **related with the geographical location of Bulgaria.** The territory of Bulgaria is a part of established trade and transport corridor between Middle East and Europe, known as “Balkan route”. The route is used for criminal purposes (traffic with people, drugs, weapons and traffic with goods and funds of legal and illegal origin). As a result of the geographical position of Bulgaria, the territory of the country is transit for different predicate offenses. The "Balkan route" also serves as a corridor for the transportation across the border of large sums of cash to and from Europe. In some cases, there is evidence of the use of systems such as „hawala” for financing terrorism purposes related to migrant flows in recent years.

The second is **related with contextual factors**, such as: the significant size of the gray economy, established levels of corruption and potential questions, related to the effectiveness of some of the competent national authorities. Another factor is related to the big percent of people under the line of the poverty. That is a factor which makes possible systemic use of strawmen in money laundering schemes is a factor of inherent vulnerability in the context of terrorist financing. Another factor which has a contextual importance is the large percentage of Bulgarians who emigrated to other countries.

SUBJECTS, INVOLVED IN THE POTENTIAL MONEY LAUNDERING ACTIVITIES:

1. Domestic natural persons

They are the biggest group of entities involved in the potential money laundering activities. In most cases. They use strawman in the schemes for money laundering which is the main method, used in the organized criminal groups. Another possible hypothesis is these domestic natural persons, acting "professional washers" and the prominent political figures. The majority of cases of money laundering is related to online fraud, usually internet scams, which are many in number but small in value. In these cases, the domestic natural persons are used as strawmen to receive/collect funds acquired through online fraud or other crimes and to transfer them abroad. The natural persons also have a serious participation in the unauthorized transfer across the border of the country of cash acquired through various predicate offenses.

2. Domestic legal entities

They are the second largest group of subjects participating in the potential activities of money laundering as the average amount of cases is significantly higher than that of the natural persons. A big part of the legal entities carry out operations with cash, which is the risk of the use of many of these entities for the investment of proceeds of crime cash into the formal financial system. Limited liability companies (LLC) are extremely vulnerable to abuse, including sole ownership (LTD), which are the simplest form of using the owner as a strawman. Complex money laundering schemes often involve legal entities registered in Bulgaria whose ownership or management is associated with offshore companies or hollow companies in other Member States.

3.Foreign natural persons

Their activities are most connected with cross-border cases of fraud (mostly computer). These events are assessed as medium risk, because despite their relatively high frequency, they currently have limited consequences. Nevertheless, strengthening the recovery mechanisms for this type of risk event will be increasingly necessary due to the digitalization of the economy and the positive growth of cyber fraud risks.

4. Foreign prominent political figures

Main risk here is using strawmen between foreign prominent political figures and foreign natural persons for money laundering of funds acquired through corruption through their investment in liquid assets or, in some cases, through participation in privatization, as well as in the Citizenship Against Investment Program (IRRC).

5. Domestic prominent political figures

They pose a high risk of money laundering, including for investment and stratification of funds abroad, incl. in offshore jurisdictions, and for their subsequent integration in the EU and in Bulgaria through a number of schemes. The consequences of activities such like this can lead to political and social instability.

HIGH-RISK SECTORS

In the NRA are indicated the high-risk sectors which are used for money laundering and financing terrorism.

Financial sectors in which are concluded other sector, such as:

1. Money in cash - they are used in the sector and businesses in connection with the commission
of the various predicate offences. That is the predominant type of property that is „laundered".

2. Formal financial system – used mainly for investment and stratification of the "laundered" funds, as the main part of them "passes" through the Bulgarian financial system, without the same being a "final" destination for integration of these funds into different financial products.

3. The bank sector – transfers in the country, cross-border transfers and cash transfers withdrawals are the methods that prevail in cases of money laundering. These funds are mainly used from domestic legal entities to facilitate the laundering of money acquired through tax offenses (including VAT-related offenses) and fraud. The main identified risk is the complex stratification of funds by foreign legal entities in cross - border aspect, including in the banking and banking products sector non-bank investment intermediation.

4. Sector of investments in financial instruments - non-bank investment intermediaries operating online trading platforms are the highest risk for money laundering internationally, due to the relatively large turnover, very wide geographical diversification and the shortcomings of absentee identification of clients, as well as and due to the formal implementation of some of the requirements of the preventive legislation against money laundering and financing terrorism.

5. Remittance services sector – concludes cross-border transfers and cash withdrawal. This sector is also highly exposed to and vulnerable to the risks of money laundering and financing terrorism.

6. The electronic money sector – this sector is posed to the risk of money laundering and financing terrorism because of the fact that there is an opportunity to remain anonymous. The risks of money laundering and financing terrorism are potentially increased in the case of new products such as „virtual currencies" due to the possibilities to remain anonymous and the lack of detailed data on their use.

7. The currency exchange sector - provides opportunities for investing funds from cash-generating criminal activities in Bulgaria.

The non-financial businesses and professions sectors

They represent a high risk because of the weak regulation of the sector and control and the relative popularity of the sector among foreigners. In the sectors are concluded persons who by occupation provide legal advice, and persons who by profession provide accounting services and / or advice in the field of taxation. Also the traders in precious metals and precious stones and articles with and from them, as well as casinos. With regard to traders in precious metals

and precious stones and articles with and from them, the risk of terrorist financing is also increased.

Economic sectors

NRA identifies a number of economics sectors that are usually used for money laundering in its various phases. The most vulnerable to money laundering economic sectors include fuels and coal mining, wholesale and retail trade retail, real estate, transport and agriculture in the context of fraud with EU funds. Small and medium-size enterprises used to be more vulnerable to risks from money laundering, as they are not subject to the same state control as larger enterprises.

Economic sectors are used for different purposes in the stages of money laundering, with the trade sector being used mainly in the context of money laundering through trade activities.

A significant part of the Bulgarian economy is dependent on the spending of state and budget funds and the award of various types of public procurement and public activities, which are associated with the possibility of misappropriation of public funds by prominent political figures and potentially involved private sector actors. In this sense, the public sector is potentially the main source of funds which can be appropriated in a criminal way and as a result of that to be invested stratified by various means.

There are several free trade areas in Bulgaria, which are a favorable environment for the risks of money laundering and financing terrorism, due to the relaxed regulatory requirements, as well as the vulnerabilities regarding the transparency of the actual ownership of the entities operating in the areas.

Activity	**Evaluation of the probability**
Money laundering from corruption	Very high
Money laundering from organized crime	Very high
Money laundering from tax crimes	High
Money laundering from fraud, incl. computer and social engineering	Average
Money laundering from drugs	High
Money laundering from people trafficking	Very high
Money laundering from contraband	Average
Money laundering through limited liability companies	Very high
Money laundering through legal entities with foreign participation	High
Money laundering through prominent political figures	Very high

5.2.Malta

The National ML / FT Risk assessment has been commissioned to identify and assess threats and vulnerabilities to which Malta has been exposed to, with particular relevance also to the identification of sectors or industries more likely to be abused or misused. In summary, the findings of the NRA can be summarised as follows:

Table 1: Summary of Malta's ML/TF threat assessment

Threat Category	Overall Threat Level	Sub-Category	Threat Level
	Medium-High	Tax Evasion	High
		Local criminal groups	High
		Drug Trafficking	Medium-High
		Fraud & Misappropriation	Medium-High
		Corruption & Bribery	Medium-High
		Smuggling	Medium
		Theft and receipt of stolen goods	Medium
Money Laundering of Domestic proceeds of crime		Armed robbery	Low
		Living of the earnings of prostitution	Low
		Usury	Low
		Illegal gambling and violations of the Gaming Act	Low
		Human Trafficking	Low
		Smuggling of persons	Low
		Unlicensed Financial Services	Low
Money Laundering of Domestic foreign proceeds of crime	High	ML of foreign proceeds of crime threat level has been calculated for a number of countries	

[33] Second proviso to Regulation 13(3) PMLFTR

Table 2: Summary of Malta's ML/TF sectoral vulnerability assessment

Sector	Sector Vulnerability		Sub-sectors	Sub-sector vulnerability		
	Inherent	Residual		Inherent	Controls	Residual
Banking	High	Medium-High	Core Domestic banks	High	Medium-Low	Medium-High
			Non-core domestic & international banks	High	Medium-Low	Medium-High

Securities	Medium-High	Medium-High	Collective investment schemes	Medium-High	Low	Medium-High
			Custodians	Medium-High	Low	Medium-High
			Foreign Exchange	Medium-High	Low	Medium-High
			Fund Administrators	Medium-High	Low	Medium-High
			Fund Managers	Medium-High	Low	Medium-High
			Stockbrokers	Medium	Low	Medium
Insurance	Medium	Medium	Insurance	Medium	Medium-Low	Medium
Other Financial Institutions	Medium-High	Medium-High	Payment Services	High	Medium-Low	Medium-High
			Lending	Medium-Low	Medium-Low	Medium-Low
			Other Activities	Medium	Low	Medium
Gaming	Medium-High	Medium-High	Land based gaming	Medium	Medium-Low	Medium-Low
			Remote gaming	High	Low	High
Designated Non- Financial Businesses and Professionals (DNFBP)	High	High	Company service providers	High	Low	High
			Lawyers	High	Low	High
			Trustees and fiduciaries	High	Low	High
			Notaries public	Medium-High	Low	Medium-High
			Accountants and auditors	Medium-High	Low	Medium-High
			Real estate agents	Medium-High	Low	Medium-High
			Dealers in high value goods	Medium	Low	Medium

5.3.The Kingdom of the Netherlands

The Dutch policy for prevention and repression of money laundering is based on the recommendations of the Financial Action Task Force (FATF) and the directives of the European Union. Member States of the FATF, including the Netherlands have committed themselves to follow the 40 FATF recommendations for the prevention and repression of money laundering, terrorist financing and measures to improve national legal systems and international cooperation in those areas. On EU level, most of the FATF recommendations

have been transposed in the 4th AML Directive. Pursuant to Article 7 of this Directive, the EU Member States must prepare risk-based policies against AML and TF and establish national risk assessment (NRA).

Money laundering can have legal and economic nature. Money laundering in the legal sense is the concealment or disguise of the real nature, origin, location, disposal or displacement of an object or the conceal or disguise who the entitled party is or who has the object in his/her possession, while there is knowledge or suspicion that the object directly or indirectly originates from a criminal activity. The economic approach describes the process and it focuses on the manner by which money interacts with criminal activities and its origin is being disguised.

According to the conclusion of the FATF in its Mutual Evaluation Report (2017), the Netherlands is particularly vulnerable to money laundering because of its open, trade-oriented economy and the fact that it has a vast and internationally oriented financial sector.

The NRA lists the top ten risks (see table below), highlighted by experts, with the greatest potential of causing money laundering in the Netherlands. Money laundering through financial institutions is the highest potential risk. Experts assess the potential risks of misuse of bank services as highest because of the large amount of money that flow through the financial sector.

Top 10 risk factors	**Level of potential impact (scale 0 - 100)**
• Money laundering via financial institutions (i.e. banks)	71-75
• Money laundering via payment service providers • Money laundering via trust offices (corporate service providers) • Money laundering via offshore entities	61-70
• Money laundering to discard hidden value • Trade based money laundering • Money laundering via tax-driven complex corporate structures • Money laundering via virtual currencies • Money laundering via cash operations • Money laundering via (inter)national investments and/or investment structures	55-60

The opinion of the experts is based on the current market "players" and it does not include the potential new market participants, such as money laundering via virtual currencies and block chain technology. These new technologies have been considered as potential new threats to the market integrity and enhancement of money laundering and terrorist financing.

The NRA also assesses the effectiveness of the applicable national and international legal framework. With regard to national laws and regulations the Wwft is the most important

instruments in the strife against money laundering and terrorist financing. The law imposes a number of obligations to financial institutions and no-financial professional groups, for example: they are obliged to investigate clients (identification and qualification of UBOs), transaction monitoring and reporting of unusual transactions to FIU-the Netherlands. Other national laws combating money laundering are: The Trust Office Supervision Act (Wtt), the Financial Supervision Act (Wft), the Taxation Act, the Dutch Criminal Code, the Integrity Promotion Act for Public Administration (Bibob), the Sanctions Act, and the Trade Register Act. On EU level, the most prominent instruments are the EU 4th and 5th AML Directives as well as the PEP Directive, which have already been implemented into national law.

The experts consulted for the NRA have concluded that in general the current legislation in place is effective and that it does not miss any significant AML elements. However, they also do not consider the available measures to be completely eliminating the risks of money laundering. According to their estimation, the current legislative instruments are on average combating around one third of the identified AML risks. Therefore, significant improvements in this direction are required. The sectors needing immediate action being, the banking sector and payment service providers.

According to the experts, the available policy instruments (and their implementation) are not sufficiently equipped to combat money laundering on a global scale. For effective prevention and repression of money laundering, a much more enhanced international cooperation and data exchange between international regulatory and supervisory authorities as well as investigative services and enforces is imperative.

In the first NRA, there was insufficient time in the experts' meetings to substantially reflect on all expert opinions and discuss the relevant case examples. This has resulted in a risk assessment with a general character. The next NRA shall focus more on the concrete examples from the practice of money laundering as well as the effectiveness of the current AML measures.

6. SANCTIONS FOR NON-COMPLIANCE IN BULGARIA, MALTA, THE KINGDOM OF THE NETHERLANDS; (TYPES OF SANCTIONS, AMOUNTS OF MONETARY SANCTIONS).

6.1. Bulgaria

The main legislative act connected with the fight against money laundering and terrorist financing is Measures Against Money Laundering Act (MAMLA). In the law are described the obliged subject, the measures they have to undertake, the regulatory authorities.

In the last chapter are pointed out the administrative – penal provisions which may be required in case of non-compliance of the measures against money laundering.

The administrative-penal provisions may be applied to anyone, who commits, or admits committing a violation, such as:

1. Non-effective application of the measures by the obliged subjects and their branches and subsidiary companies in third states;
2. Non-compliance the requirement by the issuers of electronic money and providers of payment services about creating central contact units;
3. Non-compliance the measures for complex checkup of the client by the obliged subjects in the different types of hypotheses specified in the law;
4. Non-compliance the additional measures for complex checkup of the client in the cases specified by law
5. Non-compliance the requirement by the obliged subjects to not open or maintain anonymous accounts or deposit certificates, or accounts or deposit certificates of an obviously fictitious name, as well as renting or maintaining anonymous safes or safes of an obviously fictitious name.
6. Non-compliance the requirement the obliged subjects to adopt internal rules for control and prevention of money laundering and financing terrorism. These rules shall be applied effectively also to their branches and subsidiaries abroad.

Anyone, who commits, or admits committing a violation of the provision of MAMLA and if the deed is not crime, shall be punished with a fine in the amount of BGN 1000 - 10 000 (for a natural person) or with a property sanction in the amount of BGN 2000 – 500 000 (for a legal person or sole trader).

The sanctions vary and are classified on the basis of the following criteria:

- the type of the violator – a natural person, a legal entity or person under some specific (higher risk) categories of obliged entities.

- the type of the violation.

The specific amounts of the sanctions are:

Anyone, who commits, or admits committing a violation of the law, if the deed is not a crime, shall be punished by:
1. a fine from BGN 1000 to 10 000, if the violator is **a natural person**;
2. a property sanction form BGN 2000 to 20 000, if the violator is **a legal person or sole owner**;
3. a property sanction from BGN 5000 to 50 000, if the violator is a **person under some of the categories of obliged entities** (Art. 4, p. 1 - 6 and 8 – 11).

In repeated violation, the punishment shall be:
1. the fine shall be from BGN 2000 to 20 000, if the violator is **a natural person**;
2. a property sanction from BGN 5000 to 50 000, if the violator is **a legal person or sole owner**;
3. a property sanction from BGN 10 000 to 200 000, if the violator is a **person under some of the categories of obliged entities** (Art. 4, p. 1 - 6 and 8 – 11).

For severe or systematic violations, if the deed is not a crime, the punishment shall be:
1. a fine of BGN 5000 to 2 000 000, if the violator is **a natural person**;
2. a property sanction from BGN 10 000 to 2 000 000 or to the double amount of the profit form the violation, if it may be established, if the violator is **a legal person or sole owner**;
3. a property sanction from BGN 20 000 to 10 000 000, or up to 10% of the annual turnover, including the gross revenues, according to the consolidated statement of the end parent undertaking for the previous year, consisting of receivables on interests and other similar revenues, from assets and other securities with variable or fixed revenue and receivable form commission and/or fees, if the violator is a **person under some of the categories of obliged entities** (Art. 4, p. 1 - 6 and 8 – 11).

6.2.Malta

The PMLA and the PMLFTR contemplate a number of criminal offences and administrative breaches. Criminal offences carry with them pecuniary fines and/or imprisonment, and are subject to proceedings before the criminal courts of Malta as regulated by the Criminal Code (Chapter 9 of the Laws of Malta). The criminal offences under the PMLA and the PMLFTR are listed under Section A1.5.

- Breaches of an administrative nature

The failure to comply with any lawful requirement, order or directive issued by the FIAU under the PMLFTR and the PMLA, as well as any contravention of the PMLFTR or of any procedures (including these Implementing Procedures) or guidance, may render subject persons liable to an administrative sanction. (Regulation 17 PMLFTR, Regulation 21 PMLFTR)

The FIAU is empowered to take any of the following administrative sanctions:

1. impose an administrative penalty (pecuniary sanction);
2. issue reprimands in writing;
3. instead of or in conjunction with the imposition of a pecuniary sanction or reprimands in writing, require a subject person to take any action or measure to remedy a contravention or to ensure that the subject person is in compliance with its AML/CFT obligations.

Administrative sanctions may also be accompanied by other measures, including the publication of administrative penalties on the FIAU website or notification to relevant authorities or bodies, depending on the nature of the breach.

Furthermore, administrative penalties may either be imposed as a one-time fixed penalty or on a daily, cumulative basis. In the latter case, the minimum daily penalty that may be levied is €250 per day.

- Administrative Penalties

The value of the sanctions that may be imposed for every separate contravention or failure to comply ranges from one thousand euro (€1,000) to forty-six thousand five hundred euro (€46,500).

- Serious, repeated or systematic contraventions

Notwithstanding the above, in cases of serious, repeated or systematic **contraventions** of the provisions of the PMLFTR or of any procedures or guidance (including these Implementing Procedures), the maximum sanction that may be imposed will vary depending on the activity carried out by the subject person as follows:

When the subject person carries out **relevant activity**, the maximum penalty that can be imposed by the FIAU is that of one million euro (€1,000,000), or the equivalent of twice the value of the benefit derived from the contravention in question, where this value can be quantified.

When the subject person carries out **relevant financial business**, the maximum penalty that can be imposed by the FIAU is that of five million euro (€5,000,000), or of the equivalent of 10% of the total annual turnover of the subject person, according to the latest available approved financial statements.

- Minor contraventions

Where, on the other hand, the contraventions are deemed to be minor, and the circumstances so warrant, the FIAU may impose a penalty below the aforementioned minimum threshold of one thousand euro (€1,000), but in any case not less than two hundred and fifty euro (€250). The FIAU may alternatively issue a reprimand in writing. As with all sanctions imposed, the issuance of a reprimand on a subject person will be taken into consideration by the FIAU in determining any future sanctions.

Subject Persons carrying out Relevant Activity		
Penalty for each contravention	€1,000.00	€46,500.00
Minor contraventions	€250.00*	€1,000.00
Serious, repeated or systematic breaches	€1,000.00	€1,000,000.00 or 2x the value of the benefit derived

* *This is without prejudice to the possibility of issuing a reprimand in writing rather than imposing an administrative penalty.*

- Penalties imposed on directors of a legal person

In cases where a contravention has been committed by a legal person, the FIAU may deem it more appropriate to **impose the penalty on that natural person**, who at the time of the contravention was a director or officer tasked with the responsibility for the management of the legal person, or was purporting to act in this capacity, unless that person can prove that the contravention was committed without his/her knowledge and that all due diligence was exercised to prevent the commission of that contravention.

In these instances, the FIAU may additionally communicate with the relevant authority or body responsible for the authorisation, licensing, registration or regulation of the subject person in question to recommend that action be taken to preclude that natural person from exercising any managerial functions within the subject person, as may be appropriate.

Appeals From Admnistrative Penalties

The PMLA introduces the possibility of appealing an administrative penalty imposed by the FIAU in excess of five thousand euro (€5,000), whether this amount is in respect of one or more contraventions covered by the same administrative act[36].

Subject persons may appeal from the entire penalty or from part thereof, as long as the part(s) appealed from exceed five thousand euro (€5,000), in which case the subject person is to clearly state which parts of the penalty are being appealed from. The outcome of an appeal will either confirm, vary or reverse the administrative penalty in question.

The Compliance Monitoring Committee (CMC) is an internal committee of the FIAU that is responsible to monitor and enforce subject persons' adherence with their AML/CFT obligations.

Subject persons must file an appeal application within twenty (20) calendar days of notification of the sanction letter. The application must be filed in the Court of Appeal (Inferior Jurisdiction) and the relevant provisions of the Code of Organisation and Civil Procedure[37] are to apply.

Subject persons are to note that the information and documents that form part of the appeal proceedings, including the appeal application and reply, remain confidential and, while subject persons have every right to consult a lawyer to represent them in court, the appeal will be held behind closed doors. The judgment will not be published through the usual means, save for those provisions relating to publication of penalties under the following sections.

The FIAU to publish those administrative penalties imposed by the FIAU in excess of

fifty thousand euro (€50,000) and have become final and due38. A sanction is deemed to have become final and due:

- on the lapse of twenty (20) days from the date of notification of the sanction letter and no appeal has been filed; and
- on the termination of appeal proceedings filed by the subject person, if the appeal is decided against the subject person or is withdrawn or deserted by the same.

Publication is to be carried out in accordance with the policies and procedures established by the FIAU's Board of Governors, which are available on the FIAU's website.

Notification to ESA

The FIAU is obliged to notify the relevant European Supervisory Authorities (ESAs)[39] of any administrative sanction or measure imposed on a subject person carrying out relevant financial business. In these cases, the FIAU is to notify the relevant ESA of the action taken, and is to also notify it of any appeal proceedings lodged by the subject person, and the eventual outcome of that appeal.The ESAs responsible for the supervision of entities carrying out relevant financial business are the following:

- European Banking Authority (EBA);
- European Insurance and Occupational Pensions Authority (EIOPA); and
- European Securities and Markets Authority (ESMA);

Notification to relevant supervisory authority

Whenever the FIAU imposes an administrative penalty on any subject person, it is to **inform** the supervisory authority, body or entity responsible for the authorisation, licensing, registration or regulation of, or the granting of a warrant to, the subject person in question. In doing so, the FIAU will provide all the necessary information and documentation on the contravention.

Criminal Offences under the PMLA

Article	3(1)
Offence	Money laundering.
Penalty	A fine *(multa)* not exceeding two million five hundred thousand euro (€2,500,000), or imprisonment for a period not exceeding (eighteen) 18 years, or both the fine and imprisonment.

Article	4(2) / 4B(2)
Offence	Disclosure that an investigation is taking place, or other disclosures likely to prejudice an investigation.

Penalty	A fine *(multa)* not exceeding eleven thousand, six hundred and forty six euro and eight seven cents (€11,646.87), or imprisonment for a period not exceeding twelve (12) months, or both the fine and imprisonment.

Article	4(6A)
Offence	Disclosure likely to prejudice an attachment order or a connected investigation.
Penalty	A fine *(multa)* not exceeding eleven thousand, six hundred and forty six euro and eight seven cents (€11,646.87), or imprisonment for a period not exceeding twelve (12) months, or both the fine and imprisonment.

Article	4(5) / 4(10)
Offence	Acting in contravention of an investigation order or an attachment order.
Penalty	A fine *(multa)* not exceeding eleven thousand, six hundred and forty six euro and eight seven cents (€11,646.87), or imprisonment for a period not exceeding twelve (12) months, or both the fine and imprisonment.

Article	6
Offence	Acting in contravention of a freezing order..
Penalty	A fine *(multa)* not exceeding eleven thousand, six hundred and forty six euro and eight seven cents (€11,646.87), or imprisonment for a period not exceeding twelve (12) months, or both the fine and imprisonment.

Criminal Offences under the PMLA

Article	3(1)
Offence	Money laundering.
Penalty	A fine *(multa)* not exceeding two million five hundred thousand euro (€2,500,000), or imprisonment for a period not exceeding (eighteen) 18 years, or both the fine and imprisonment.

Article	4(2) / 4B(2)
Offence	Disclosure that an investigation is taking place, or other disclosures likely to prejudice an investigation.
Penalty	A fine *(multa)* not exceeding eleven thousand, six hundred and forty six euro and eight seven cents (€11,646.87), or imprisonment for a period not exceeding twelve (12) months, or both the fine and

	imprisonment.

Article	4(6A)
Offence	Disclosure likely to prejudice an attachment order or a connected investigation.
Penalty	A fine *(multa)* not exceeding eleven thousand, six hundred and forty six euro and eight seven cents (€11,646.87), or imprisonment for a period not exceeding twelve (12) months, or both the fine and imprisonment.

Article	4(5) / 4(10)
Offence	Acting in contravention of an investigation order or an attachment order.
Penalty	A fine *(multa)* not exceeding eleven thousand, six hundred and forty six euro and eight seven cents (€11,646.87), or imprisonment for a period not exceeding twelve (12) months, or both the fine and imprisonment.

Article	6
Offence	Acting in contravention of a freezing order..
Penalty	A fine *(multa)* not exceeding eleven thousand, six hundred and forty six euro and eight seven cents (€11,646.87), or imprisonment for a period not exceeding twelve (12) months, or both the fine and imprisonment.

Criminal Offences under the PMLFTR

Regulation	7(10)
Offence	False declaration, false representation or the production of false documentation by a customer or person purporting to act on the customer's behalf.

Penalty	A fine *(multa)* not exceeding fifty thousand-euro (€50,000), or imprisonment for a period not exceeding two (2) years, or both the fine and imprisonment.

Regulation	16(1)
Offence	Prohibited disclosures (tipping off).
Penalty	A fine *(multa)* not exceeding one hundred and fifteen thousand euro (€115,000), or imprisonment for a period not exceeding two (2) years, or both the fine and imprisonment.

6.3.The Kingdom of the Netherlands

Administrative penalties: for most violations of the core Wwft obligations, the assigned regulator can impose administrative penalties that may vary from EUR 10,000 (minor violations) to EUR 4,000,000 (serious violations). The maximum penalty for banks, trust offices and a few other financial institutions such as investment firms amounts to EUR 5,000,000. In case of recidivism within 5 years from a previous violation, the administrative penalty can be twice the aforementioned amounts. Moreover, in case of serious violations by banks, trust offices and financial institutions, the Wwft provides for administrative penalties of up to 20% of the net turnover of the previous fiscal year.

Criminal penalties: According to the Dutch Criminal Code, depending on the type of money laundering, the maximum penalties for private individuals vary from:

- Imprisonment: three months (for simple culpable money laundering) to eight years (habitual money laundering).
- Fines: EUR 21,750 to EUR 87,000.

The maximum penalties for legal entities (fines only) vary from EUR 87,000 to 10% of the annual turnover of the previous fiscal year. For instance, in 2018 the Dutch Public Prosecution Service (DPPS) conducted a criminal investigation to ING bank in relation to money laundering in the VimpelCom case. The bank reached a settlement with DPPS for violation of the Wwft and culpable money laundering. According to DPPS, the bank did not prevent the bank accounts of ING customers in the Netherlands from being used to launder hundreds of millions of euros between 2010 and 2016. ING paid a fine of EUR 775,000,000.

In addition, convicted individuals can be removed from (i) rights such as holding (certain) offices, serving with the armed forces, being counsel or judicial administrator, and (ii) the exercise of the profession in which the crime was committed (Article 420 of the DCC).

According to Article 70 of the DCC, depending on the type of money laundering, the statute of limitations varies from six years to 20 years.

V. RELEVANT JURISPRUDENCE, CASE-LAW

Bulgaria

1. **Decision № 968 of 22.06.2020 under Adm. n. d. № 2302/2020 of the District Court - Plovdiv**

‘The company has the status of an obligated person under Art. 4, item 3 of the MAMLA, as it is a financial institution within the meaning of the Credit Institutions Act. In carrying out its activities, the company provided consumer loans.

The violation is expressed in the fact that the obligated person was obliged to identify the borrower under the concluded Loan Agreement before concluding it before concluding a

contract according to the requirements of MAMLA - by presenting an official identity document and taking a copy of it.

The applicant considered that there had been no violation, as they had been collected from the certificate of permanent residence, which, according to the applicant, was an official document issued by the Ministry of the Interior.

Instead of carrying out identification by requiring an official document, the financial institution has taken a copy only of an EU citizen's residence permit. According to the MAMLA, the residence documents and the SUMP are not official identity documents, due to which a property sanction in the amount of BGN 5,000 has been imposed on the company.

The court stated that the company's liability had been properly engaged. The sanction provision of Art. 116, para. to the minimum provided by law.

The court held that the indication of the city of Plovdiv only as the place of the violation was sufficient to assume that the requirement to indicate the date and place of the violation had been complied with.

The main purpose of the MAMLA is to establish measures for prevention of the use of the financial system for the purposes of money laundering, as well as the control of their implementation, as well as the provision of full information about the identity of clients - individuals.

Upon the re-inspection carried out by the court regarding the possibilities for application of the provision of art. 28 of ZANN, the court finds that the committed violation is not distinguished by a lower degree of public danger than the other violations of the same type. The elimination of the infringement in the course of the inspection cannot be accepted as a ground for the applicability of the cited provision, insofar as the deficiencies found were eliminated only in the course of the inspection and not at an earlier stage before the inspection.'

2. **Decison № 946 of 02.07.2020 under Adm. № 1545/2020 of the District Court - Varna**,

"The company has the status of an obligated person under Art. 4, item 3 of the MAMLA, as it is a financial institution within the meaning of the Credit Institutions Act. In carrying out its activities, the company provided consumer loans.

The violation is expressed in the fact that the obligated person has not identified his client under a Loan Agreement before concluding it in the manner described in the MAMLA. The client presented only a residence permit and not an official identity document. During the inspection, several more loan agreements were established, the conclusion of which also did not comply with the legal requirements for identification.

Instead of carrying out identification by requiring an official document, the financial institution has taken a copy only of an EU citizen's residence permit. According to the MAMLA, the residence documents and the SUMP are not official identity documents, due to which a property sanction in the amount of BGN 5,000 has been imposed on the company.

The court stated that the company's liability had been properly engaged. This responsibility is inherently innocent and represents the objective responsibility of the obligated person for non-fulfillment of obligations to the state and is always realized.

Following an appeal by the financial institution, the cassation instance also found that the stated cassation arguments were unfounded. In addition, the objections in the appeal have already been considered and discussed by the District Court - Varna, as they are identical to the appeal. Administrative Court - Varna fully shares the motives of the District Court.

3. Decision № 75534 of 23.04.2020 under Adm. n. d. № 14500/2019 of the Sofia District Court

With a Penal Decree a property sanction in the amount of BGN 2,000.00 / two thousand / was imposed on a legal entity and a violation under the Money Laundering Measures Act (‘LMML’).

The company is an obligated person, as its subject of activity includes the provision of consulting, accounting, information and other services.

The obligated entity has not fulfilled the obligation to identify the representatives of the company - client when establishing a business relationship.

Upon verification of the submitted documents, it was established that the Company provides processing of primary accounting documentation, preparation of accounting documents and balance sheets, preparation of annual financial statements, monthly filling in of bank documents for rent payment, insurances and taxes to the budget. At the time of establishing the relationship between the two companies, no identity documents or other official documents certifying an official personal identification number or other element establishing their identity, as well as the country of their permanent residence and address of the client's legal representatives were presented.

The decree has been revoked. The drafter and the sanctioning body have incorrectly applied the substantive law. The court points out that the violation was committed on 01.01.2015 and the liability of the Company is incorrectly committed for a violation committed on 28.12.2018. The court points out that the invoice issued on 28.12.2018 is for already provided accounting services. In other words, the two Companies had a business relationship from before that date.

The Court refers to the Law on Administrative Violations and Penalties and points out that in the present case the law that should have been applied is the old Law on Measures against Money Laundering, repealed in 2018, as business relations between the parties have begun. in 2015. Admitted both when indicating the date of the violation and when indicating the applicable substantive law.

The infringement could not be remedied in the judicial review proceedings of the penal decree, as only at this stage of the applicant's administrative proceedings would a completely new

charge be brought, both as regards the date of the infringement and as regards the infringement. legal provision.

For this reason, the court finds that the appeal is well-founded and the penal decree should be annulled.

4. Decision № 192442 of 07.09.2020 under Adm. n. d. № 5299/2020 of the Sofia District Court

'A penal decree was confirmed, by which a property sanction in the amount of BGN 5,000.00 was imposed on the grounds of violation of the Law on Measures for Money Laundering / 'MAMLA' / .

The company has the status of an obligated person within the meaning of Art. 4 item 3 of the MAMLA, as it is a financial institution within the meaning of the Credit Institutions Act.

As an obligor, the complainant did not identify a client-borrower by presenting a copy of an official identity document before concluding a consumer loan agreement. The contract is concluded through the official website of the Company.

The company stated that with regard to the client, his identification was carried out in accordance with the Internal Rules, and that the utilization of the loan amount took place against the presentation of an original identity document.

The provisions of the MAMLA regulate two stages of a complex assessment of the clients, which include first identification of the clients and subsequently - verification of their identification. According to Art. 53 para. 1 of the MAMLA, the identification of the natural persons is carried out by presenting an identity document and taking a copy of it. The norm of art. 53 para. 7 of the MAMLA stipulates that when the identification is performed without the presence of the identifiable natural person, the identification may also be performed by presenting a copy of an official identity document.

According to Art. 15 para. 1 of the MAMLA, the measures for complex verification of the clients / including their identification and verification of the identification / are applied before the establishment of business relations. In this case, the loan agreement was concluded in the absence of the person subject to identification, therefore the identification of the client should have been done by presenting a copy of an official identity document / identity card, passport, SUMPS - § 1 item 12 of RD of MAMLA supra art. 13 ZBLD /.

The Court finds unfounded the applicant's objection that the client had a previous legal relationship with him and is not subject to re-identification. The court points out that any new consumer credit agreement constitutes a new business relationship, before the establishment of which the financial institution has the obligation to apply the measures of complex verification to the client. Respectively - by repaying the utilized loan, the legal relationship between the parties is repaid. When concluding a consumer loan agreement, not only is there a presumption for the duration of the legal relationship, but given the nature of the loan agreement, the

borrower's obligation is periodically performed, ie. the legal relationship will continue to exist for the term of the contract.

The court also pointed out that although the legal theory set out by the applicant the considerations for the real nature of the loan agreement under the CPA, the presentation of an original ID card by the client upon utilization of the amount in cash at EasyPay was not relevant to the fulfillment of the financial institution's obligation to identify the client precisely by means of a copy of an official identity document.

Regardless of the presentation of a copy of the client's ID card in the course of the administrative penal proceedings, it is established with certainty that a copy of the same was not presented before the conclusion of the consumer loan agreement of 02.01.2019.'

5. **Decision № 229 of 16.07.2020 under Adm. № 522/2020 of the District Court - Montana**

'With the decision was confirmed a penal decree imposing a pecuniary sanction on a company for violation of the Law on Measures for Money Laundering ("LMML"). The decision was confirmed by a decision of 16.11.2020 under c.adm.n.d. № 428/2020 of the Administrative Court - Montana.

The company has the status of an obligated person under Art. 4, item 3 of the LMML, as it is a financial institution within the meaning of the Credit Institutions Act.

The violation is expressed in the fact that as an obligated person the financial institution should have identified its client under a Loan Agreement before concluding it, according to the requirements of Art. 53, para. 1 of the LMML, namely - by presenting an official identity document and taking a copy of it.

Instead of carrying out identification by requiring an official document, the financial institution has taken a copy only of an EU citizen's residence permit. According to the LMML, the residence documents and the SUMP are not official identity documents, due to which a property sanction in the amount of BGN 5,000 has been imposed on the company.

The court points out that the LMML obliges its addressees, including financial institutions, to apply the measures for complex inspection of clients when establishing business relationships. These measures are for preventive purposes and aim to prevent abuse.

The cassation instance also found that the act was not committed incidentally. On the contrary - such an act was committed in the identification of three other individuals, and the non-sanctioning of these violations in the manner prescribed by law is irrelevant. Subsequent actions performed by the company to identify the persons do not change the factual circumstances of the act, as the administrative violations have already been committed.'

6. **Decision of 22.04.2021 on k. adm. n. d. № 47/2021 of the Administrative Court - Sliven**

In the Decision is discussed imposed property sanction Insurance company for violation of the Law on Measures against Money Laundering ('MAMLA').

The Insurance Company has the status of an obligor under Art. 4, item 5 of the MAMLA, as he is an insurer who has received a license under the conditions and by the order of the Insurance Code.
The violation is expressed in the fact that the obligated person has not identified a legal representative of his client when concluding an insurance contract.

The court stated that the identification of a client was done by presenting an identity document and taking a copy of it. Instead, when concluding the insurance contract, the insurer presents a residence certificate of an EU citizen. Referring to §1, item 12 of the LMML, according to which the residence documents and the SUMP are not official identity documents, the court accepts that the obligated person has not fulfilled his obligation for identification.

The court reduced the sanction imposed from BGN 20,000 to BGN 5,000, as it held that the violation had not been committed systematically by the insurer. According to the MAMLA, it is a systematic violation that has been committed by an obligated person five or more times.

Malta

Final judgements delivered by Maltese Courts on money-laundering offences have been somewhat sparse. Over the past years however, there have been a steady rise in arraignments and indictments concerning alleged money-laundering offences, albeit, as of date of report, proceedings remain sub judice, for a number of reasons, including but not limited to constitutional references.

At the outset, it must be noted that although a Maltese court shall, in the delivery of judgement, make reference to a number of sources, including jurists, and judgements delivered by the European Court of Justice or by local courts, there is effectively no doctrine of legal precedent. This effectively means that a Maltese court of Law is not bound by the findings, conclusions and inferences which may have been drawn by a Maltese court, differently presided, thereby allowing the sitting judge or panel of judges wide discretion in delivering judgement. A Maltese court of law may therefore reinforce the findings of a previous judgement, or ostensibly disregard it with diametrically opposite findings.

Based on the aforesaid premise, it is nevertheless possible, through an analysis of judgements delivered by Maltese Courts, to identify the over-arching themes2 that have been consistently addressed and reinforced over time.

Maltese Case Law

1. The link to the Predicate Offence

The definition of money-laundering hinges on a process whereby the illicit proceeds derived from a criminal activity are concealed or disguised in order to give the aforesaid proceeds a

legitimate appearance. An essential element therefore is that the proceeds derive from a predicate offence – the proceeds of which are then laundered. Judgements delivered by Maltese Courts have sought to expand upon the requisites of predicate offences, with particular emphasis on the concepts of stand-alone (or autonomous) money laundering and third-party laundering.

In self-laundering prosecutions, proving the link to the predicate offence is often seen as less difficult as it is most likely that the offender is charged in Court together with the crime that generated the illicit funds hence the link to the predicate offence is evident.

On the other hand however, when stand-alone (or autonomous) money laundering or third-party laundering is prosecuted, the link to the predicate offence may not be as evident. This presents the prosecution with a more onerous task in linking the money allegedly laundered as having been derived from a predicate offence.

The necessity for a link to a predicate offence to the money laundering charge has, almost inevitably, resulted in a number of conflicting judgements. Consequently, legislative changes were introduced that sought to significantly dilute the aforesaid link to predicate offences, to one where the prosecution is only required to provide evidence prima facie between the link between the money or property and the predicate offence.

To further bolster this notion, the amended Article 2(2)(a) of the PMLA now states that a prior conviction in relation to a predicate offence, does not necessarily hinge on a final conviction on money laundering, insofar that the prosecution can prove, through circumstantial evidence, the link between the money allegedly subject to money laundering and the predicate offence.

This point was succinctly addressed by the Court, in Police v. Sharon Camilleri4, whereby the Court held:

'[…] even though the underlying criminal activity is not proven, if the prosecution manages to prove that the source of the funds originates from a criminal activity, then the criminal activity would have been proven and there would not be the need of prove in relation to a final judgment in connection with a criminal offence.'

In Police v. Vincent Etienne Vella5, the Court further stated that:

'(…)the Prosecution are aided, to a degree, in proving the necessary crime originator of the questioned laundered proceeds by direct evidence where available, or by circumstantial evidence or any other evidence, and need not necessarily produce an actual conviction that establishes the underlying offence. Neither does the Law require them to proof with precision the nature of the crime involved.'

Whilst, the onus of proof required from the prosecution may appear to have been substantially lightened, the Courts are still very cautious in applying this provision, as evidenced in Republic of Malta v. John Vella6:

'(…) Not every acquisition, not every conversion of transfer of a property, not every disguise or showing of property necessary amounts to money laundering. This law is extraordinary and introduces a radical concept in our local system which requires acute application and attention so that it is not converted into a tool of injustice, which seem to be more reminiscent of the inquisition age rather than the modern days of human rights.'

2. Shifting the Burden of Proof

Another interesting theme that has been consistently examined in local judgements is the burden of proof necessary to support a successful money laundering prosecution, with particular emphasis on the interplay between Article 3(3) and Article 22(1c)(b) of the PLMA. The aforesaid matter has been at the centre of recent court judgements – whereby the conclusions drawn was that insofar that the prosecution is able to prove, on a prima facie basis, the link between the proceeds of crime allegedly laundered and the predicate offence, then the burden of proof is shifted onto the accused to prove the legitimate origin. This was explained by in detail by the Court of Criminal Appeal in Police v. Carlos Frias Mateo (Police v. Carlo Frias Mateo, decided on 19th January 2012, Pg. 7) whereby the Court stated that:
'Therefore, the level of proof at a prima facie level applies also for the person accused of money laundering […...], all the prosecution has to prove is that the money that were found in possession of the person were not in conformity with the lifestyle of the person which proof can be established even from indicative proof.

This means that the prosecution need not prove to the Court the origin of the funds, or whether the funds are illegal. All it has to prove on a prima facie level is that there is no logical or plausible explanation in relation to the origin of the funds. Once this is done it is the turn of the accused to ascertain the legality and origin of the funds.'

This 'prima facie' requirement to reverse the burden of proof, remains a divisive and strongly debated notion. It has been espoused in other judgements and staunchly denounced in others. The aforesaid provision appear to be incompatible with time-honored legal precepts, some of which are entrenched in the Constitution notably, the presumption of innocence. Furthermore, the burden of proof has, bar in very select circumstances, been always attributed to the prosecution, who must, in criminal proceedings, secure a prosecution based on the highest probatory value i.e. beyond reasonable doubt.
The reversal of the burden of proof as well as the dilution of the probatory value to prima facie, undoubtedly stems from the practical difficulties that a prosecution would face when probing predicate offences, some of which may stem several years, and involve cross-border transactions.
The aforesaid difficulty has been the catalyst underpinning significant legislative changes, which have sought to shift the burden of proof onto the defendant a point, examined by the Court of Criminal Appeal in the judgement below:
'There is no doubt that the crime of money laundering is one of the most difficult and delicate crimes which can be subject to an investigation. The technique and sophistication of the way in which the money is routed and disguised to hide its illicit origin makes it almost impossible for the investigators to trace the origin of the funds. It was because of this that in these circumstances Money Laundering Law, Chapter 373 shifts the burden of proof on the subject, in so much that it is the subject who has to prove to the satisfaction of the Court the legitimate origin of the funds which were found in his possession.' (Ibid, Pg. 8)

The prima facie requirement as a trigger to the shifting of the burden of proof, was further explained in Police v. Alfred Delia (Police v. Alfred Delia, decided on 23rd May 2013, Pg. 27) whereby the Court clarified that: '(…) was the "prima facie" level satisfied? Was there a case to answer so that the burden of proof shifts on the accused that he is required to prove the origin of the utilised funds.'

3. The principle of ne bis in idem in the context of ML

The objective of the principle of ne bis in idem (also referred to as 'double jeopardy') is to ensure that no person is prosecuted on the same identical charge twice, a principle staunchly entrenched in the Charter of Fundamental Rights of the European Union (Article 50). The main thrust for argument where is whether the arraignment to face predicate offences should coincide with the money laundering charge, or should the money laundering charge be presented at a secondary stage, whether this is effectively a breach to the ne bis in idem principle.
Recent Court judgements appear to have examined the point through a differentiation between self-laundering, stand-alone (or autonomous) money laundering and third-party laundering.
The conclusions drawn is that in the event of self-laundering, the charge of money laundering should be added to the list of charges straight away, although this is not a pre-requisite as the PMLA allows in Article 2(2)(b) for a person to be charged separately for both the money laundering offence and for the underlying criminal activity.
With regards to third-party laundering, inevitably the party charged with the money laundering is not the party involved in the criminal activity generating the proceeds of crime.
Therefore any challenges to the ne bis in idem concept may arise when a person is charged with self-laundering proceeds from his own criminal activity separately. This point was examined by the Court of Criminal Appeal in Republic of Malta v. Christian Grech (Republic of Malta v. Christian Grech, decided on 12th December 2013, Pg. 16/17), whereby the Court stated that:
' The defence is arguing that there is an 'overlapping' between the income originating from the prostitution (which is part of the crime) and the money laundering. However, with all due respect this is not legally correct. In money laundering, one is accused to have converted or transferred property knowing it originates from criminal activity or that he disguised or hid the true origin of the funds, place and disposition of the property and that he knew that could have directly or indirectly originated from criminal activity.

[……..] The elements of the second offence are totally different from the elements of the first offence. What follows is that there is no overlapping between what the accused is being accused of in other procedures and the crime of money laundering. The facts are totally and unequivocally different and since these are totally different facts then there cannot be a case of 'ne bis in idem'.

Thereby, the Court of Criminal Appeal refuted the principle of ne bis in idem as a defence for when an individual is charged with the underlying criminal activity separately from when he is charged with money laundering.

The Kingdom of the Netherlands

1. The Netherlands Supreme Court dated 9 July 2019, alternative scenario :

The Court of Appeal based its conviction on the indirect method of proof. In short it means that an accused can be convicted of money laundering even though the predicate offence from which his illegal (and laundered) earnings originated from, is unknown: the Court only needs to exclude any legal source of origin. This can be done by following six steps.

So first of all, there is no specific predicate offence to connect to the laundered objects. Second, whether there a suspicion of money laundering. If so, how does the accused respond when confronted with this suspicion; fourth, can the accused provide a statement that is concrete and more or less verifiable – and not highly unlikely? Fifth, if that's the case, police and the Public Prosecution Service are obliged to further investigate this statement. Sixth, based on the outcome of such an investigation the Court has to decide whether the accused statement is valid: if not and a lawful origin can be excluded, the accused can be convicted of money laundering.

In this particular case the accused had three bank accounts in which cash sums totaling more than € 300,000 were deposited over the course of about six years. During the appeal the question arose whether the accused's statement on the origin of this amount was sufficiently concrete and verifiable and not highly unlikely. With respect to the origin of the money, the accused stated that he had acquired large sums of money from, inter alia, property sales, revenue from a snack bar, poker winnings, rent and the sale of figurines and gold. The accused kept the money at home and, on occasion, at his friends'. Money would sometimes also be deposited in bank accounts, with a view to make payments that required bank transfers. Investigation into his tax returns showed that the accused did not have any income or assets which could explain the cash deposits. Nor did the accused submit any evidence that showed a record being kept of the cash flows. The accused has not given any substantiation or explanation with regard to the cash flows that led to the cash deposits in the three bank accounts. The Court of Appeal thus concludes that the accused has not in any way provided a statement that is both concrete and verifiable in terms of the origin of the cash deposits. It therefore determines that there is no need for further investigation of the accused's statement and convicts the accused of money laundering. The Supreme Court does not deem the Court of Appeal's judgment to be incomprehensible since the cash flow was not made transparent, either prior to and during the period found.

The accused was sentenced to a 12-month imprisonment.

2. Overijssel Court, 13 February 2018, cash in rolled chicken meat :

The suspect has emerged during a money laundering investigation, aimed at co-suspects in Aruba. The investigation showed that the suspect spoke in veiled terms with co-suspect X about moving large amounts of cash. Subsequently in Aruba a sea container was seized in which a cash amount of €2,833,340 was found in boxes with chicken products. The sea container was shipped by company A, of which the suspect was the sole shareholder. When the suspect was arrested in Aruba he stated that he was not only involved in this money transport, but also in an earlier transport of €4,000,000. The money allegedly originates from co-suspect Y.

According to the court the transport of two large cash amounts justifies the suspicion of money laundering. Because of the way in which the money was transported (and the security risks involved) and because it is a well-known fact that various forms of crime involve large amounts of cash. The suspect did not give a statement explaining the origin of the cash. This means that the court reaches the conclusion that the amounts of money must originate from crime. According to the court the suspect laundered the two amounts of money, totaling €6,833,340.

Among other things, the Public Prosecution Service also charged the suspect with laundering an amount of €975,000. According to the court, the case showed that company A supplied meat products to (among others) company E (established in Bulgaria). A part of the invoices, however, was issued in the name of company B (established in Panama). As a result, it seems as if company B supplied meat to company E, whereas the business accounts show that everything was supplied by company A. This means that the invoices (to the amount of €972,579) to company B are false and that the flows of money –therefore- originate from crime. Company B subsequently provided loans to the amount of €975,000 to companies C and D (both established in Bulgaria). This means possession and turning over of money originating from crime. The investigation shows that all the companies involved are affiliated with the suspect. Therefore, the court imputes all the acts between the companies to the suspect and as a result he is considered to be the perpetrator of money laundering.

Misuse of trade flows to move values may indicate trade based money laundering. Criminal money is moved internationally through trade and is given a seemingly legal origin. In this case it is unclear whether the €972,579 was criminal money or that it concerned a tax structure. The court dismisses that question and argues that the money had a criminal origin from the moment that company B paid company E as a result of false invoices.

The suspect is also convicted of laundering €309,000 and €17,000. Considering the duration and frequency of the acts the court is of the opinion that it concerns habitual money laundering.

3. Court of Justice in The Hague, 15 September 2017: Money laundering by filing a tax return

This was a case where fraud in medical expenses was brought to light. False invoices were made up in which more hours were charged than had been given in treatment. A substantial portion of the amounts that were deposited in the bank account of the health care provider in question carne from payments of criminal origin. The suspect (managing director of the health care provider) used the bank account for making payments for the purchase of a house and a car.

The judge ruled that this was a case of money laundering, seeing that these purchases were (in any case partially) financed by money from criminal activities, and it was no longer possible to trace whether, and if so to what degree, they had been combined with legally obtained funds. The suspect argued that income tax had been paid over the extra hours that had been invoiced. According to the judge, the fiscal declaration of that income can be interpreted as an act of concealment and considered punishable as a form of money laundering.

The standpoint that filing a tax return gives the income as it were the appearance of legality, and thus constitutes money laundering on its own, is open to discussion. This is certainly the case given the fiscally valid concept 'fiscal neutrality': in principle, for income tax purposes it is not important whether the income has been earned by criminal actions or not. In this case, however, it does seem as though there was a substantial act of concealment that is closely related to fraud: invoices were made up for treatment that had not been delivered, the invoices were entered in the accounting system, and the income so generated was reported to the Tax and Customs Administration. In addition, several parties collaborated in carrying this out. The

question remains whether, in a case like this, the charge of money laundering has some kind of added value when money laundering is so closely related to the predicate offence.

4. The Court of Appeal of The Hague, dated 24 October 2018, seizure of bitcoins :

In a criminal case, the Dutch Public Prosecution Service has had to return a large amount of bitcoins as it could not be proven that these had been 'mined' via stolen electricity. The Court of Appeal rules that in respect of the return in principle the value of the bitcoin at the time of the seizure is decisive. In this matter, 157,000 euros had to be returned, the value of the Bitcoin at the moment of seizure. While the amount would have been 3.3 million euros, had the exchange rate upon the moment of the return of the bitcoins been decisive.

The suspect mined bitcoins using equipment that was generated with stolen electricity. The computer that had been seized on 18 February 2014 was found to have a bitcoin wallet. The first investigation into the computer on 20 February 2014 showed that the wallet had a balance of 127 bitcoins. Further investigation on 23 October 2014 and following synchronization with the bitcoin network showed that the wallet turned out to have a much higher balance, namely a total of 712 bitcoins. These 712 bitcoins are subsequently seized and sold by the Public Prosecution's Service on 24 October 2014.

The Court of Appeal establishes that the suspect has mined a total of 127 bitcoins during the period in which the electricity was stolen. These are confiscated. The Court of Appeal cannot establish a relationship between the other 585 bitcoins that had been seized and the theft of electricity and ordered for these to be returned to the suspect.

Upon calculating the value of the 127 forfeited bitcoins, the Court of Appeal starts with the basic premise that the value of the bitcoin is as it was at the time of the actual moment of seizure. The Court of Appeal sets the exact moment of valuation in the present case at one week after the seizure of the computer. This one week is considered to be a reasonable period for an investigation into the computer and for the disposing of the bitcoins, thus the Court of Appeal. Subsequently, the Court of Appeal derives the value at that moment in time (date seizure + 1 week) from 'publicly available (internet) sources', taking into account the average value on that day. In this case, this was about 500 euros per bitcoin. Meaning that 127 bitcoins with a counter value of approximately 63,500 euros are to be forfeited.

The 585 bitcoins that have to be returned were not seized and actually removed from the control of the seized party until October. As those bitcoins had been disposed of very shortly afterwards, the amount that the disposing actually generated is taken as a point of reference for calculating the value of those 585 bitcoins: approximately 270 euros for each bitcoin.

5. Criminal bitcoins and money laundering

In November 2017 two investigations dealing with the conversion of criminal bitcoins into cash were brought before a Dutch court. The first investigation covered a drug dealer who operated via Darknet; the drugs were paid for in bitcoins, and the bitcoins were then converted into cash using a bitcoin dealer. The bitcoin dealer guaranteed anonymity in return for a high commission. The court ruled that by using a bitcoin dealer, the criminal origin of the bitcoins had been concealed.

In the second investigation the bitcoin dealer himself was put on trial. The dealer bought up large quantities of bitcoins that had been earned on Darknet, sold these through regular markets, and received a high commission. The court's premise was that practically all bitcoins from the Darknet have a criminal origin. An expert's investigation demonstrated that nearly exclusively illegal goods are traded on Darknet and that the only payment is with bitcoins. Given the high commission, the dealer must have known about the origin of the bitcoins, since 'a legal economic motive is lacking for selling bitcoins at the rate employed'.

In this investigation a bitcoin mixer also came up for discussion. Bitcoins paid out on Darknet had been mixed and then turned into cash. The reason for the use of a mixer was to conceal the origin of the bitcoins, the court said.

The judgements are in line with the money laundering typologies recently established in the Netherlands for monitoring the trade in virtual forms of payment and the use of a bitcoin mixer.

6. Zschüschen, ECHR indirect method of proof

The Dutchman Zschüschen opens a bank account in Belgium in March 2003 and deposits a total amount of € 75.000 in 5 transactions within 2 months. Zschüschen has a history of drug trafficking and no income (in the Netherlands). A money laundering case is started against him in Belgium. Initially, he states that the money was earned with untaxed (undeclared) work during a 4-year period. He does not want to give the names of employers. During the entire proceedings he claims the right to remain silent. In 2006, Zschüschen is sentenced in Belgium (10 months' suspended sentence, a € 5.000 penalty and confiscation of the € 75.000).
The legal questions:

Zschüschen first of all relies on article 6, par. 1 and 2 of the ECHR. More specifically on the breach of the right to a "fair trial", the presumption of innocence and the right to remain silent. The fact that the predicate offence is not specified during the proceedings, allegedly is a breach of his defence rights as well as a breach of the right to be informed promptly about the charges. In addition, article 6, par. 3(a) ECHR is also relied on.

In summary, the conclusion of the ECHR is that Zschüschen loses the case on all counts.

7. Self-laundering

Section 420bis.1 of the Dutch Criminal Code reads as follows:
"Money laundering that consists of no more than acquiring and or being in possession of an object that originates directly from a person's own criminal activity is punishable with a maximum term of imprisonment of six months or a fourth-category fine."

Prior to the penalization the situation of being in possession or acquiring an object that directly originates from a person's own criminal activity usually resulted in discharge from prosecution if no actions to disguise the criminal origin were taken. The Supreme Court argued that merely acquiring and being in possession of an object that originates directly from a person's own criminal activity does not necessarily qualify as money laundering. For the qualification 'money laundering' the suspect must have performed an act aimed at hiding or concealing the criminal origin of the object in question.

The Explanatory Memorandum states that the raison d'être of self-laundering lies in the prevention of impunity. The impression had been created that the qualification-ground for exclusion too often led to impunity if the predicate offence could not be proven.

Recently the first judgment in which the new self-laundering article was proved was published . Some of the details of this case are discussed below.

The suspect committed fraud. The suspect approached the victims via Whatsapp where he presented himself as a relative or close acquaintance of the victim. The victim would be persuaded to transfer large amounts of money to account numbers belonging to straw men. After the amounts of money had been deposited the suspect would receive the money from the straw men.
According to the Court, as from that moment the suspect was in possession of money that originated from his own criminal activity. The evidence does not show that the suspect performed acts to hide/conceal the criminal origin after receiving the money. Therefore, the proved facts cannot be qualified as money laundering and, therefore, the qualification-ground for exclusion applies, in the Court's opinion. It is noteworthy that the Court does not regard the use of straw men as an act aimed concealing the criminal origin. It seems that the Court regards this as part of the fraud itself.

But, the Court argues, article 420bis.1 of the Dutch Criminal Code came into force on 1 January 2017. As a result, the possession of an object that originates directly from a person's own criminal activity is penalized in the form of self-laundering. The laundering took place after the date of coming into force. Therefore, the Court does consider it proved that the suspect committed self-laundering.

Declaring both the basic offence and the (culpable) self-laundering proved may lead to discussions about the application of the convergence rule. The Supreme Court suggested to charge the suspect with (culpable) self-laundering in the alternative to the predicate offence in order to prevent convergence. The first thing that is notable about this judgment is the fact that the Public Prosecution Service did not charge the self-laundering nor, therefore, the element 'from a person's own criminal activity'. As a result, the element 'from a person's own criminal activity' also does not reappear in the declaration of proved facts. In addition, the Court considers both the basic offence and the self-laundering of the proceeds of the fraud proved, but it does not address the possibility of convergence. In sentencing, the Court only appears to take into consideration the sophisticated nature of the fraud, the number of victims and the straw men who were not aware of the fact that their bank accounts were misused by defrauding people. It is unclear whether declaring the self-laundering proved has increased the sentence.

8. ING Bank and VimpelCom

Dutch bank ING Groep NV admitted criminals had been able to launder money through its accounts and agreed to pay EUR 775 million to settle the case.
"The shortcomings identified resulted in clients having been able to use their bank accounts for money laundering practices for years", ING said in a statement, after signing one the largest ever such settlements in the Netherlands.

Dutch financial crime prosecutors said ING had violated laws on preventing money laundering and financing terrorism "structurally and for years" by not properly vetting the beneficial owners of client accounts and by not noticing unusual transactions through them.

The fine is not ING's first for failing to prevent illegal transactions. In 2012 it paid a penalty of $619 million for facilitating billions of dollars-worth of payments through the U.S. banking system on behalf of Cuban and Iranian clients.

In the latest case, which had led to questions from regulators in the United States, Dutch prosecutors said they had begun their investigation in 2016 after realizing that a pattern of violations was a signal of deeper underlying problems at ING.

They cited four examples where ING accounts were used for crime, most notably for bribes paid by telecommunications company VEON, formerly VimpelCom, in Uzbekistan. Veon settled U.S. and Dutch charges for $835 million in 2016.

"We had various ongoing criminal investigations and ING bank accounts cropped up repeatedly", Frohberg said in a telephone interview. "Since 2008, ING was repeatedly warned, but it failed to take sufficient measures to stop the practice."

Some of the shortcomings the Dutch authorities found in the bank's AML transaction monitoring system are:

- The settings on the transaction monitoring system limited monitoring on some accounts.
- Monitoring was conducted at the account rather than the customer level, preventing an integrated review of all activities by a given customer.
- The transaction monitoring system's settings limited the number of alerts generated per account to 3 a day. This limit was apparently set to keep the transaction review workload for compliance personnel manageable.
- The settings looked at only percentage changes in activity, not the total value involved, so that the system did not identify a pattern of improbably high-value transactions. For example, transactions worth €150 million passed through the account of a customer identified as an "underwear trader."

The significance of these shortcomings is that they were essentially technical, and could presumably be remedied by "simply" changing the relevant settings. Of course, expanding the universe of transactions monitored, and the number of alerts generated, would require committing additional resources to process and review all the new information. The Dutch government's conclusion was that, in at least some cases, the settings were deliberately set so as not to overwhelm the personnel available, precisely because there weren't enough personnel to handle a larger number of alerts.

9. Anti-money laundering and counter-terrorist financing measures in The Netherlands and in Ukraine

This case is about a trust company which provides trust services to natural persons and legal entities. The trust company provided her services to a natural person who owned real estate in Ukraine (person A). The real estate was worth USD 10,000,000. Person A issued certificates of the real estate portfolio to a legal entity (entity B). The shares of entity B were held by a

nominee shareholder of Ukrainian nationality (person C). Therefore, person C was the ultimate beneficiary owner of the real estate portfolio. At a certain moment, person C transferred his shares to another person (person D). Person C did not receive anything in return for these shares, they were transferred to person D free of charge. Person A informed the trust company about the transfer of shares and the trust company appointed person D as the new ultimate beneficiary owner of the real estate.

A few months later, the trust company informed the Dutch Financial Investigation Unit (FIU) of several transactions, including the transfer of shares mentioned before. This is when the problems arose. After being informed of the transfer of shares from person C to person D, the Dutch National Bank (DND) imposed a fine of EUR 40,000 on the trust company. Reason for this was failure to comply with the Wwft. According to DNB, the trust company should have suspected that the transfer of shares could be related to money laundering or terrorist financing, since the shares were transferred free of charge while the real estate portfolio was worth a lot of money. Therefore, the trust company should have reported this transaction within fourteen days, which derives from the Wwft. This offence is usually punished with a fine of EUR 500,000. However, the Dutch National Bank has moderated this fine to an amount of EUR 40,000 because of the extent of the offence and the track record of the trust company.

The trust company took the case to court because she believed the fine was imposed unlawfully. The trust company argued that the transaction was not a transaction as described in the Wwft, since the transaction was supposedly not a transaction on behalf of person A. However, the Commission thinks otherwise. The formation between person A, entity B and person C was constructed in order to avoid a possible tax collection from the Ukrainian government. Person A played a key role in this construction. Furthermore, the ultimate beneficial owner of the real estate changed by transferring the shares from person C to person D. This also involved a change in the position of person A, since person A no longer held the real estate for person C but for person D. Person A was closely involved with the transaction and therefore the transaction was on behalf of person A. Since person A is a client of the trust company, the trust company should have reported the transaction. Furthermore, the Commission stated that the transfer of the shares is an unusual transaction. This lies in the fact that the shares were transferred free of charge, while the worth of the real estate represented USD 10,000,000. Also, the worth of the real estate was remarkable in combination with the other assets of person C. Lastly, one of the directors of the trust office pointed out that the transaction was ‘highly unusual’, which acknowledges the strangeness of the transaction. The transaction therefore arises suspicion of money laundering or terrorist financing and should have been reported without delay. The fine was therefore imposed lawfully.

10. A present of 8 million euros (ECLI:NL:CBB:2018:6) – failure to report on time an unusual transaction

A trust office had failed to report a transfer of shares /depositary receipts for shares in time to FIU-Netherlands and consequently received an administrative penalty.

This judgment was rendered by the Dutch Trade and Industry Appeals Tribunal (College van Beroep voor het Bedrijfsleven) on 17 January 2018. Earlier, the court had come to the same conclusion.

DNB had imposed an administrative penalty of 40,000 euros on the trust office since the office had not reported the above transfer to FIU-Netherlands until four months later.

The case started in December 2013 when a client, who had only recently been accepted by the office, reported the matter. Without any consideration, 8 million euros worth of property, placed with a legal entity organized and existing under the laws of the Seychelles, had been transferred to another party. It was not until April 2014 that the trust office reported the transfer to FIU-Netherlands.

The Tribunal agreed with DNB that, because of several suspicious aspects to the transfer, the trust office should have reported the transfer without delay as laid down in the provisions of Wwft. The penalty of 40,000 euros has therefore been confirmed.

Sources

1. Best Practices for counteraction of Monel Laundering, manual for the employees of Sofia Municipality, Risk Monitor;
2. Money Laundering through commercial deals, Finance 3/2014 XVII;
3. Crimes against the Tax and Insurance system, Guidelines for investigation, Chamber of the Investigators in Bulgaria;
4. Investigation of Money Laundering, Guidelines, Chamber of the Investigators in Bulgaria;
5. Prevention of Money Laundering, Risk and typological approach, Risk Monitor;
6. Strategy for counteraction of Money Laundering in Republic Bulgaria 2011-2015; American Gaming Association;
7. Anti-Money Laundering and Combating the Financing of Terrorism Bulgaria, Report on Fourth Assessment Visit, 2013;
8. Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorism financing affecting the internal market and relating to cross-border situations, European Commission, 2017;
9. Risk and Compliance Report Bulgaria, 2018, knowyourcountry.com;
10. Money Laundering in Bulgaria: State of Affairs and policy Implication, Policy Brief No. 69, May 2017, Center for the Study of Democracy;
11. Exploring and Industry - Wide Standard to Customer Risk Assessment – Proposing a Best Practice Model for Banks, Advancing Financial Crime Professionals Worldwide;
12. The FATF Recommendations, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, June 2019, FATF;
13. The Forty Recommendations, FATF;
14. Anti-Money Laundering and counter Terrorist financing for judges & prosecutors, June 2018, FATF;
15. Best Practices Paper, October 2012, FATF;
16. Best Practices on Beneficial Ownership for Legal Persons; October 2019, FATF;
17. Money Laundering / terrorist financing risk and vulnerabilities associated with gold, July 2015, FATF;
18. Money Laundering and Terrorist Financing through trade in diamonds, October 2013, FATF;
19. Money Laundering Through the Physical Transportation of Cash, October 2015, FATF;

20. National Money Laundering and Terrorist Financing Risk Assessment, February 2013, FATF;
21. Professional Money Laundering, July 2018, FATF;
22. Virtual Currencies Key Definitions and Potential AML/CFT Risks, June 2014, FATF;
23. Good Practices on the Prevention of Money Laundering and Terrorist Financing in the Notarial Sector, 2018;
24. The Round Detailed Assessment Report on Bulgaria, Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, 2008 MONEYVAL;
25. Manual for Implementation of Measures from AMLA and Regulations for application of AMLA for Prevention of Abuse with New Technologies, Products and Transactions that Could Lead to Anonymity; 2012, State Agency for National Security;
26. Guidance for establishment and reporting of Suspicious Transactions/Operations/Client under AMLA which Could Be Connected with Irregularities and Fraud with EU Funds;
27. National Risk Assessment for Bulgaria 2020;
28. Report from the Commission to the European Parliament and the Council assessing the framework for cooperation between Financial Intelligence Units, 2019, European Commission;
29. Study on Best Practices in vertical relations between the Financial Intelligence Unit and law enforcement services and Money Laundering and Terrorist Financing Reporting entities with a view to indicating effective models for feedback on follow-up to and effectiveness of suspicious transaction reports, 2007/2008, European Commission;
30. Measures against Money Laundering as counteracting of the corruption practices in public procurement, VUZF;
31. Instructions for reporting under the AMLA, 2012, State Agency for National Security;
32. The Risk Factors Guidelines, 2017;
33. Identifying Money Laundering in Business Operations as a Factor for Estimating Risk, Volume 3, Issue 3, August 2017, International Journal of Innovation and Economic Development;
34. Understanding Money Laundering through real estate transactions, 2019, European Parliament;
35. Guidelines on the Identification of Suspicious Financial Transactions for Financial Dealers, 2003, Indonesian Financial Transaction Report and Analysis Center;
36. Money Laundering Awareness Handbook for Tax Examiners and Tax Auditor, 2009, OECD;
37. Risk of Money Laundering through Financial Instruments, Users and Employees of Financial Institutions, 2010, UNODCl;
38. Best Practices for Anti-Money Laundering Compliance 2019-2020
39. Financial Markets Anti-Money Laundering Act (amendment 62/2019) – Austria;
40. Federal Public Service Economy, SMEs, Self-Employed and Energy, Federal Public Service Home Affairs, Federal Public Service Justice and Federal Public Service Finance – Belgium;
41. https://iclg.com/practice-areas/anti-money-laundering-laws-and-regulations/belgium;
42. https://www.nbb.be/en/financial-oversight/combating-money-laundering-and-financing-terrorism/analysis-atypical-3;
43. Anti-Money Laundering and Terrorist Financing Law (8/11/2017) – Croatia;
44. Monetary and Financial code – France;

45. https://gettingthedealthrough.com/area/50/jurisdiction/28/anti-money-laundering-france/;
46. https://complyadvantage.com/knowledgebase/aml-regulations-france/;
47. https://www.fatf-gafi.org/publications/mutualevaluations/documents/mutualevaluationoffrance.html
48. https://www.amf-france.org/en/professionals/management-companies;
49. Interpretation and Application Guidance in relation to the German Money Laundering Act – Germany;
50. https://www.lexology.com/library/detail.aspx?g=cceab5bc-8264-4ae0-9ad2-7a5622de6533;
51. Prevention and Suppression of the Legalization of Proceeds of Crime and Terrorism Financing (Government Gazette No. 139/30.07.2018) – Greece;
52. Act LIII of 2017 on Prevention and Combating of Money Laundering and Terrorist Financing – Hungary;
53. Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Updated to 2 December 2019) – Ireland;
54. Law on the Prevention of Money Laundering and Terrorist Financing – Lithuania;
55. Prevention of Money Laundering and Funding of Terrorism Regulation – Malta;
56. Act On Counteracting Money Laundering and Terrorist Financing – Poland;
57. https://dre.pt/web/guest/pesquisa/-/search/108021178/details/maximized;
58. law no. 129/2019 to Prevent and Combat Money Laundering and Terrorism Financing, as well as to amend and supplement some legislative act – Romania;
59. Law 10/2010 of 28 April, on the prevention of money laundering and terrorist financing – Spain;
60. https://www.lansstyrelsen.se/stockholm/other-languages/english/businesses/society-and-development/money-laundering.html;
61. https://www.fi.se/reporting-to-the-financial-intelligence-unit#fk;
62. A Beneficial Ownership Implementation Toolkit, 2019, OECD;
63. Guide to Beneficial Ownership Information: Legal Entities and Legal Arrangements, G-20 Anti-Corruption Working Group;
64. Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems;
65. Guidance for a risk-based approach: Virtual assets and virtual asset services providers.