Università
Ca'Foscari
Venezia

Master's Degree
in Management

Final Thesis

Customer Due Diligence challenges and the evolution of European AML legislation

Supervisor
Ch. Prof. Andrea Minto

Assistant supervisor
Ch. Prof. Marco Palmieri

Graduand
Giovanni Castriani
Matriculation number 851268

Academic Year
2019 / 2020

To my family

Table of Contents

List of abbreviation

AML	Anti-Money Laundering
AUI	Archivio Unico Informatico
BO	Beneficial Owner
CDD	Customer Due Diligence
DD	Due Diligence
EBA	European Banking Authority
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
GAFI	Gruppo di Azione Finanziaria Internazionale
GDP	Gross Domestic Product
GPML	Global Programme against Money Laundering
IMF	International Monetary Fund
KYC	Know Your Customer
ML	Money Laundering
OECD	Organization for Economic Co-operation and Development
OS	Ownership Structure
PEP	Politically Exposed Person
RBA	Risk Based Approach
STR	Suspicious Transaction Reporting
TF	Terrorist Financing
UBO	Ultimate Beneficial Owner
UIC	Ufficio Italiano Cambi
UIF	Unità di Informazione Finanziaria
UN	United Nations
UNODC	United Nations Office on Drugs and Crime

INTRODUCTION

Money laundering and terrorism financing are two crimes which have been suffering a significant growth of attention over the latest years, influenced by economic and historical factors led by technologic innovations. The relevance of these themes and the consequences that these themes have had all over the world forced the world institutions to respond with the aim to fight the phenomena. The European Union anti-money laundering commitment started in the first years of the nineties and the laws and regulations implemented have been constantly updated over the years. As it will be covered later in this thesis, the European Directives were first developed following a rule-based approach. From 2003 the International Institutions identified the risk-based approach to be the best one to address the ML and TF problems. The regulators' task was very difficult, they have had to develop a sort of common anti-money laundering "culture" among the obliged entities and its employees. The employees' continuous training has been a key characteristic for the accurate application of the rules, even if it required lots of effort and time.

The current AML framework is quite complicated and developed. It is composed by the International Recommendations issued by the Financial Action Task Force and, as regards the European Union, by a Directive (at the time of writing this thesis the V Directive has been published) which implemented the FATF Recommendations into Community law. Each EU Member State has to transpose the Directive into National law, because only through a transposition into national law the EU rules can be applied. The aim of this thesis is to investigate the evolution of the AML scenario in Europe and its transposition in Italy presenting the five European Directives, focusing on the customer's due diligence and understanding its core concepts.

CHAPTER I: MONEY LAUNDERING

1.1. What is money laundering?

In the latest years Anti-Money Laundering discipline captured, progressively, more and more attention among the whole globe. Why is it happened only in the last years? AML discipline has been present in Italy and in the European Union since 1991 and it has been updated year by year, as we will specifically see in chapter 2, with the European Directives history. Anti-money laundering is becoming more and more important due to the growing awareness of the negative consequences that the phenomena have on government, state, people and companies. The distortions that money laundering causes to the markets are too many to be ignored by States and their people. The world and the markets globalization, technological innovations and the increasing complexity of financial products and investment services, represent a strong trend facilitating money laundering operations on a transnational basis. Money launders usually adjust their laundering methods focusing on the less supervised sectors. The role of banks in the fight against money laundering, because of their central and crucial position in financial market, has taken the shape of an encompassing and above all very intrusive system[1]. But when legislation started to aim attention on the banking sector, criminal shifted to the insurance industry. When the insurance sector started to be regulated against money laundering, criminals moved into real estate. This sort of game continues, and money laundering keeps expanding

[1] *The anti-money laundering complex and the compliance industry,* Routledge, A. Verhage, 2011.

into even more sectors[2]. The direction taken by the several countries involved in the illegal processes was aimed toward an efficient collaboration based on common principles as transparency, collection and exchange of information, according to a preventive and proactive attitude towards risk. Basing on these assumptions governments and international institutions are increasing their focus on finding new and more efficient ways with the aim of reducing and fighting money laundering activities. The control regime in the latest years, as we will cover later in the customer due diligence evolution chapters, has extended from the banks and financial institution, the original subjects, to a wide range of businesses (such as the casinos, jewelers, insurance companies and others)[3]. Nowadays these businesses are required to play an active role against money launderers.

Money laundering is an interdisciplinary phenomenon that can be seen in lots of different models. For example, it can be seen as a complex schema where different types of financial institutions, intermediaries, accountants and advisors based in different countries are involved, against the law, to launder their client money. But to understand deeply the phenomenon with all its facets we must consider it as a simple concept: it is the process through which criminals hide the illegal provenience of their capital through investment or legitimate financial operation allowing them to be used within the legal economy. Money laundering is a so-called *second degree* offense, which concerns the proceeds of other criminal activities. Following Stessens (2000), Levi and Reuter (2006) "persons who engage in money laundering do this to avoid punishment and to be able to benefit from their profits through investments and consumption in the legal economy"[4]*.* In this way criminal organizations have the possibility to invest and spend "legally" the money earned during their illegal practices, such as drug trafficking[5]. Doing so, criminals have the possibility to improve their control and

[2] *Transnational Organized Crime*, analyses of a global challenge to democracy, Transcript Verlag, C. Jojarth.

[3] Money Laundering, M. Levi and P. Reuter, *Crime and Justice,* Vol. 34 2006, The University of Chicago Press.

[4] *The anti-money laundering complex and the compliance industry,* Routledge, A. Verhage, 2011.

[5] Following *Vienna Convention* (United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988) guidelines, drug trafficking is the only crime related

diversify their investment (through the legal economy), resulting in a cycle where they will always gain more and more power. The criminals' ability to use both the legal and illegal economy, combined with the relation of legal and illegal activities, gives to criminal organizations greater benefits than illegal activity alone[6]. From a criminal's perspective money laundering process is the fundamental step of their activity, without money laundering criminals couldn't be able to reinvest their illegal earnings in the economic system because if they do it, with the current laws, they will be identified by police forces and prosecuted. As we will see after, nowadays the identification[7] of the physical person who is going to operate through the financial system is one of the fundamental themes of the money-laundering regulation.

Money laundering can be defined in various forms but the most part of most of the countries adopted the definition of the Article no. 6 of the United Nations Convention Against Transnational Organized Crime (Palermo Convention, December 2000)[8]:

- "The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action;

- The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;

- The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;

---

to Anti-money laundering offence. Other crimes as kidnapping or theft under *Vienna Convention* cannot constitute money laundering offences.

[6] *The anti-money laundering complex and the compliance industry,* Routledge, Antoinette Verhage, 2011.

[7] Through the "Customer Due Diligence" procedure.

[8] As we can understand from the "Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism", *The International Bank for Reconstruction and Development/The World Bank/ The International Monetary Fund,* 2006.

- Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article."[9]

Following Betti (2001), "the UN Convention, attended by 120 countries, represents the first attempt to include in one single binding document all the concepts and measures necessary to fight organized crime on a global scale"[10]. Money laundering definition developed a lot over the years, initially the UN Convention definition coincide with the first EU Directive one. Both European instruments and the UN Convention describe money-laundering offences as those committed intentionally, but some suggestions have been made for including also the concept of negligence' among the elements of crime[11]. Despite the money laundering definitions, their effectiveness may be severely reduced if the law says that money laundering can be punished only if the proceeds originate from a limited number of crimes (usually the offences are considered to be drug-related). The EU regulators began to move towards to include a wider range of crimes in the definition, making money laundering more punishable regardless the predicate offences.

Thus, a more current definition was released by European regulators in the fifth EU Directive, that define as money laundering the following conduct when committed intentionally:

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,

[9] General Assembly 55/25 *United Nations* Convention Against Transnational Organized Crime, January 8th, 2001.

[10] *The European Union and the United Nations Convention against Transnational Organized Crime*, working paper, S. Betti, European Parliament, 2001.

[11] *The European Union and the United Nations Convention against Transnational Organized Crime*, working paper, S. Betti, European Parliament, 2001.

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)."[12]

Usually, money laundering was associated with typical criminal organization activities, but nowadays it is also correlated to bribery, fraud and tax evasion. The most recent money laundering technique mainly use banks and other financial institutions[13], operating often in tax havens or in countries characterized by high banking secrecy, in order to ensure the anonymity, key element for the entire money laundering operations. Some of these recent money laundering techniques also exploit the international financial markets potentiality, in which the daily transaction volume has such high value that money laundering operations may be unnoticed.

1.2. The Money laundering process

Money laundering processes are often composed by several operations. These multiple operations usually took place in different countries because in this way it is more difficult for criminals to be detected. The laundering phase can be also

[12] EU Directive no. 2018/843 of May 30th, 2018.

[13] Such as insurance company, currency exchange and money transfer services, etc.

carried out in offshore countries with strong banking confidentiality laws[14], thus money launders can be completely "invisible" to their authorities. As aforementioned money laundering begins with the fruits of a crime, the underlying or predicate offense such as drug sales, and ends with funds that can be used for any purpose[15]. The criminals have a multitude of different money laundering schemes, and all these schemes have in common that they aim to dissociate the criminal proceeds from their dirty origins and to create a false legitimate appearance through a series of transactions[16]. Despite of the advantages of money laundering, it is considered a very costly method. The money laundering costs is estimated at around 50 per cent of the amount of money that is to be laundered[17]. Usually[18] for each money-laundering process we can recognize three different phases: *Placement*, *Layering* and *Integration*, this three-stage segmentation can be useful to simplify the money laundering process; the process can be seen in a sequence or alone, and sometimes it could be difficult to define in which specific phase the process is[19].

- *Placement.* The first phase involves the placement of illegal proceeds into the financial system. This step is often made operating through financial institutions, casinos, shops and other businesses both in the domestic and international markets. Launderers mostly prefer to transfer dirty money where financial institutions are not strict about reporting large cash deposits to the authorities[20]. Usually during this phase, the money has its closest connection with crimes and there are less chance that the true sources of the funds have been obscured. There are numerous methods to inject cash into the system: money launderers, for

[14] *Banking Secrecy and Offshore Financial Centers,* Money laundering and offshore banking*,* M. Young, Routledge, 2013.

[15] *Crime and Justice,* Vol. 34, M. Levi and P. Reuter, The University of Chicago Press, 2006.

[16] *Transnational Organized Crime*, analyses of a global challenge to democracy, C. Jojarth, Transcript Verlag.

[17] *The anti-money laundering complex and the compliance industry,* Routledge, A. Verhage, 2011.

[18] Not all money laundering transactions involve all the described three phases, and some may involve also more (Van Duyne and Levi, 2005).

[19] *Responding to Money Laundering International Perspectives*, E. U. Savona, 2005.

[20] *Money Laundering and Terrorist Financing Activities*, F. Milan and A. E. Kurce, Business Expert Press, 2016.

example, can deposit a small amount of money (under the reporting bank threshold) over time into different banks (or in different offices of the same bank) and then put back together the money into one account. This system of dividing criminal proceeds into smaller parts is the so-called *"smurfing"* process, which is often used at this stage to avoid detection. Money launderers can also move the money abroad and deposit it in foreign countries with softer regulations, or they can purchase high-value goods (as art objects, metals and precious stones) which can be resold through checks or wire transfers payment. Sometimes bank collaboration may be present; when bank employees are corrupted, intimidated or controlled, the placement process can be easier. This collaboration makes high volume cash deposit uncomplicated, in particular when customer reporting rules, which we will cover later, are discretionary rather than mandatory[21].

In short, the solutions used to achieve the goal (move liquid money into bank accounts) are numerous and it is up to the imagination of money launderers always to find new ones.

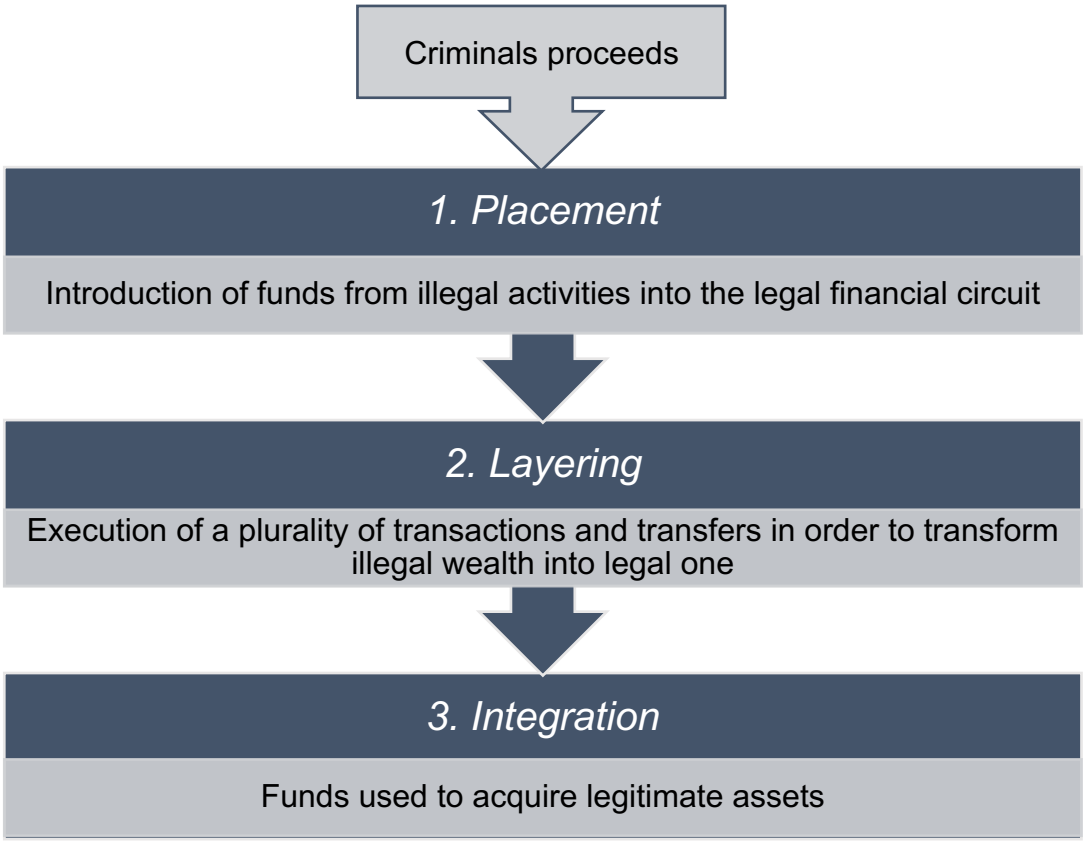
- *Layering.* The second phase begins once the placement phase is terminated. When criminal proceeds have been introduced in the financial system, money launderers need to create one or more layers of financial transaction in order to hide and separate money from their criminal source. Doing so, after multiple financial transactions that can be also made through offshore states, the funds provenience is completely covered. Trying to reconstruct the funds trail is almost impossible. The transaction with the aim of hiding the money provenience can be made through an easily transferable financial instrument, as securities or insurance contracts and through negotiable instrument[22].

[21] *Responding to Money Laundering International Perspectives*, E. U. Savona, 2005.

[22] *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism*, The International Bank for Reconstruction and Development/The World Bank/ The International Monetary Fund, 2006.

- *Integration.* This is the third phase of the money laundering process. In the integration phase criminal funds are introduced into the real economy in forms that appear normal. For example, the money laundered can be introduced in the real economy through the deposit of sums deriving from sales of goods, real estate transaction, sale of securities or redemptions of policies; it is not important how the money is introduced, from money launders' perspective they have to make it impossible to identify the origin of their funds. Ad example, money launders, with the assistance of banking confidentiality laws in offshore financial centers, are able to complete successfully the integration phase[23]. In this way criminals have the possibility to spend or invest the money laundered, "cleaned" from any connection with the previous criminal activities, following their needs.

Graph nr.1: The money laundering process



[23] *Banking Secrecy and Offshore Financial Centers,* Money laundering and offshore banking, M. Young, Routledge, 2013.

The extent to which money launders develop new money laundering techniques to conceal their criminal proceed, to convert it into other form of assets and to create a legitimate appearance depends directly on the extent to which they face a real risk of detection and sanction by police authorities[24]. Criminals also would always search for a weakness of the systems in financial institution[25]. Therefore, rules and regulations are the key factors for fighting money laundering. If the law did not criminalize money laundering, the criminals will not launder their money anymore because they would have no reason to waste their proceeds.

1.3. Why should we fight money laundering crimes?

As said before, money laundering implies lots of different negative consequences on the country's economy and on their social texture. All money laundered represents many resources taken away from the country's economic development and from the citizen's well-being. Actually, a study on 17 OECD industrialized countries mentioned in the report *"Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes"* published by the United Nations Office on Drugs and Crime (UNODC), identifies that for each billion of US dollars laundered the country economic reduces its growth by 0,03 – 0,06 percent. Despite that estimate it is extremely difficult to assess the dimension of the money laundering damage. Following Christine Jojarth (2013) on money laundering, "the most immediate threat is the undermining of efforts to combat crime and terrorism with negative consequences for a country's security and political stability. More indirect, but by no means less

[24] *Transnational Organized Crime*, analyses of a global challenge to democracy, Transcript Verlag, C. Jojarth, 2013.
[25] *Money Laundering and Terrorist Financing Activities*, Milan Frankl and Ayse E. Kurce, Business Expert Press, 2016.

severe, is the threat money laundering poses to economic development as a result of its distorting effect on investment decisions and competition"[26]. The kind of damage that police forces can cause to money launders is higher if it is referred to the laundering process than to their core activity. A seizure of money and assets are not as easily replaceable as drugs because it requires much more time and much more knowledge. Since the 90's the Government's strategy was to fight criminal organizations starting to focus against money laundering schemes. According to Mary Young (2013), "the International confiscation law is central to fighting transnational crimes because it targets the immense profits made by organized criminals"[27]. The policing tactic of "*follow the money*" used by the investigation authorities to find the perpetrator, is rendered ineffective when the money trail is successfully obfuscated through a web of complex transactions[28].

Following Joras Ferwerda's study (2008) "the empirical estimation shows that the crime level in a country can be reduced by improving anti-money laundering policies, especially if it focuses on international cooperation. This is most likely due to the international character of money laundering. This result should be an extra incentive for countries and international organizations to continue (or start) with their efforts to promote and develop the international cooperation in the fight against money laundering to decrease the amount of money laundering and crime worldwide"[29]*.* In addition, also Donato Masciandaro (1995) demonstrate in his study[30] that more sever the anti-money laundering policies are, consequently minor the money launderers' proceeds are. Then the legislators have to find out a balance between the anti-money laundering policy effectiveness and that policies costs, trying to reach an optimal policy effectiveness level with the lowest costs (for the obliged entities). Thus, it is extremely important that all countries understand the money laundering cost and adopt specific laws to prevent and

[26] *Transnational Organized Crime*, analyses of a global challenge to democracy, Transcript Verlag, C. Jojarth, 2013.

[27] *Banking Secrecy and Offshore Financial Centers,* Money laundering and offshore banking*,* M. Young, Routledge, 2013.

[28] *Transnational Organized Crime*, analyses of a global challenge to democracy, Transcript Verlag, C. Jojarth, 2013.

[29] The Economics of Crime and Money Laundering: *Does Anti-Money Laundering Policy Reduce Crime?,* J. Ferwerda, Tjalling C. Koopmans Research Institute, Utrecht School of Economics, November 2008.

[30] *Economia del riciclaggio e della politica antiriciclaggio,* D. Masciandaro, Giornale degli economisti e annali di economia, EGEA SpA, Aprile-Giugno 1995.

fight it. The Governments' aim should be to focus on the citizen's well-being, and criminal activities are an obstacle because criminals promote uncertainty and therefore insecurity about the future[31].

1.4. Some numbers to understand the dimension of the phenomena

Money Laundering is a very difficult phenomenon to quantify due to its nature. By definition it leads to secrecy, criminals who usually perform money laundering crimes don't need to register and promote the importance and volume of their operations. Furthermore, nowadays money laundering operations take place on transnational bases, so they are extremely difficult to identify and trace. In this context also trying to make some estimates on the phenomena is very difficult and with high error margins. However, many international organizations tried to estimate the volume of money laundered around the globe.

The first institution which attempted to estimate the laundered money was the Financial Action Task Force (FATF), they started from the total amount of drug sold in the US and in Europe. During the second part of the 1980s the amount of drug sold was equal to 124 billion of US dollars and basing on those data they compute that 85 billion of US dollars (equal to 0,5 percent of the world GDP for that year) could be used for money laundering operations. The step forward for the FATF was to assume that the amount of drug sold was representing just a quarter of the total amount of criminals' global income, so they set the percentage of the global money laundered to the two percent of the global GDP. Basing on

[31] Rey, 1995.

the 2009 world GDP data[32], following the FATF estimate, the amount of money laundered in 2009 was equal to **1,2 trillion** of US dollars.

The International Monetary Fund in 1998 also attempted to estimate the amount of total money laundered in one year around the world. Their research, one of the most generally quoted, resulted in finding a "consensus range" between two and five percent of the world gross domestic product as the amount of money laundered. Relying on the IMF evaluation, for the year 2009[33], the amount of money laundered was between **1,2 and 2,9 trillion** of US dollars.

A more recent study, published in 2011[34], was made by the United Nations Office on Drugs and Crime (UNODC) collecting different types of estimates. They determined that the total of the criminal income (for one year) appear to be around the three-point six percent of the world GDP, always taking the 2009 as a reference it is equal to 2,1 trillion of US dollars. Based on the criminal income estimates they identified the amounts of money laundered as the two-point seven percent of the world GDP, equal in 2009 to **1,6 trillion** of US dollars. In this more recent estimate, the percentage of money laundered is located to the lower part of the mid-nineties IMF "consensus range". But the UNODC study took a step further, they determined also the percentage of transnational criminal income equal, following their studies, to the one-point five percent of global GDP, corresponding in 2009 to 870 billion of US dollars. Basing on this estimate they deduced that the amount of money available to be laundered, in a transnational context, was equivalent to 580 billion of US dollars corresponding to the one percent of the world GDP. Thus, in conclusion, actual estimates indicate that if we consider the transnational or international context, the money available to be laundered would be equal to the one percent of world GDP, under the IMF "consensus range".

[32] As reported by World Bank the global GDP was equal to $60.39 US trillion in 2009.

[33] As reported by World Bank the global GDP was equal to $60.39 US trillion in 2009.

[34] Research Report *"Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes",* United Nations Office on Drugs and Crime, October 2011.

It is important to underline that all these estimates and studies are useful to have an indicative order of magnitude[35] of the money laundering phenomena. As aforementioned, it is extremely difficult to have an accurate evaluation.

1.5. Terrorism financing

When we refer to "Terrorism financing" we are referring to any activity aimed to the collection, accumulation, intermediation, deposit, custody and distribution of economic resources to finance and support actions "with terrorism purpose". In 1999 the United Nations (UN) convened an International Convention for the Suppression of the Financing of Terrorism and tried to define it in Article no. 2:

1. “Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

    a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or

    b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an

[35] Reuter, Truman, 2004.

international organization to do or to abstain from doing any act.

2. …

3. For an act to constitute an offence set forth in paragraph 1, it shall not be necessary that the funds were actually used to carry out an offence referred to in paragraph 1, subparagraphs (a) or (b).

4. …

5. …"[36]

In the financing of terrorism, the offences are represented by the purpose of the investment of economic resources, as they are used to finance illegal terrorist activities. It is not necessary that the money used to finance terrorism is laundered money, it is an offence also providing legal money to terrorism organizations. But of course, there is a strong link between terrorism financing and money laundering. Terrorist organizations have to cover the source of the money collected (legal or not) due to the fact that money covered should be available for the future and their activities can continue undetected[37]. Thus, the technique adopted to hide the funds source are the same that are used by money launders.

[36] *International Convention for the Suppression of the Financing of Terrorism* adopted by the General Assembly of the United Nations in resolution 54/109 of December 9th, 1999.

[37] *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism*, The International Bank for Reconstruction and Development/The World Bank/ The International Monetary Fund, 2006.

CHAPTER II: HISTORIC ARGUMENTATION AND ANTI-MONEY LAUNDERING FRAMEWORK

2.1. Historic Argumentation on Anti-Money Laundering discipline

In Italy we had a historic know how on money-laundering discipline due to the high level of importance that Italian criminal organization, as mafia, had in the country. So, since the early nineties an Italian Magistrate, Giovanni Falcone, understood that the most efficient way to hit the criminal organization was on their financial side. In the second half of the XX century the world development brought us lots of changes, a growth in the internationalization of product and consumption and an increasing interconnection between international markets led us on a reduction on anti-money laundering regulation due to the increased difficult to identify the subject involved, the way they move their capital and where[38]. At international level in 1989, during the Economic Summit of Industrialized Countries held in Paris, the seven most industrialized countries of the summit decided to develop and international way to face money laundering problems implementing international standards[39]. The result was the institution of the Financial Action Task Force (FATF), an intergovernmental body which has the purpose to develop strategies to combat money laundering and, from the 2001, also prevention of terrorism financing[40]. As a result, in 1991 the FATF

[38] Rey, 1995.

[39] *Banking Secrecy and Offshore Financial Centers,* Money laundering and offshore banking*,* M. Young, Routledge, 2013.

[40] Starting from 2008 the FATF mandate has also been extended to fight the financing of the proliferation of weapons of mass destruction.

published a report with forty Recommendations for reducing money laundering activities. Coming back to Italy, in 1991 Falcone was the father of the first Italian anti-money laundering law[41], and it was articulated in three parts: the first one contained the typical AML norms; the second one improved the list of the supervised entities (because if the only supervised entities were the banks criminals could operate through other financial entities without being controlled) and were implemented a "non" otherwise supervised financial entities register[42]; the third one contained lots of different and various norms on numerous aspects of the fight against anti-money laundering. In the first part three AML fundamentals were listed: all the operation over twenty million of Lire, or other currency, had to be made through the banking system[43]. All the operation over the previous threshold must be registered (also through the identification of the person who make the transaction) from the bank in a specific archive[44]. If a bank had the suspect that an operation could be part of a money laundering process it had the obligation to report the suspicious transaction[45].

This first Italian anti-money laundering law was the basis of the First European Anti-money Laundering Directive[46]. The first EU Directive was released just months later after the conversion of Italian AML law. With this practice European institutions applied for the whole European states the "Italian" regulation trying to unify the European countries' effort against the money laundering practices. The EU first Directive proved from the beginning its effectiveness, but in Italy the second part was removed from the national AML regulation because it was included in the Consolidated Law on Banking. Italian regulation was operative for two years before the enter into force of the EU Directive so the Italian institution developed their own regulation, surpassing the European one, and published in 1997 a new Legislative Decree correcting some limits of the previous one. This

[41] Law no. 197, July 5th, 1991 (that converted the Legislative Decree no. 143/ 1991).

[42] To join the register there were some prerequisite (ex. company managers cannot be sentenced for usury), but the aim of the register was only to record the financial entities presence. The entities were not really "supervised", they were just registered so police force know which specific entities was doing financial business.

[43] Art. 1, Legislative Decree no. 143, of May 3rd, 1991.

[44] Art. 2, Legislative Decree no. 143, of May 3rd, 1991.

[45] Art. 3, Legislative Decree no. 143, of May 3rd, 1991.

[46] EU Directive 91/308 of June 10th, 1991.

novel Legislative Decree introduced new entities[47] subjected to AML regulation, trying to involve all the subjects that could promote or perform money-laundering crimes.

As happened before, in 2001 European Union published the second AML Directive[48] based on the updated Italian regulation. However, the second Directive expanded the new entities subjected to AML regulation surpassing for the first time Italian law. As we will see in the chapter 4.2 the new included entities are the legal and accountant professions[49]. Therefore, having Europe increased the entities subjected to AML norms, Italy needed to transpose the second Directive into national law[50]. Thus, the European Union was trying to standardize, at least for European countries, the anti-money laundering regulation and was also working on the continuous development of the norms. Following the FATF Recommendations in 2005 the third EU Directive[51] was introduced by European Parliament. As we will see after, through this Directive the European Union makes FATF Recommendations mandatory for all the European countries. For the first time also the prevention of the use of the financial system for the purpose of terrorist financing was introduced in the Directive. As done with the previous Directive Italy needed to transpose the third one in the national law. Italy transposed firstly the Directive section referred to the prevention of terrorist financing with the Legislative Decree no. 109 of June 22nd, 2007 and then the Anti-money laundering section with the Legislative Decree no. 231 of November 21st, 2007. The Legislative Decree no. 231 is considered the Anti-money laundering Italian regulation collection. Why did Italy transpose the third EU Directive into different laws? The Italian Government wanted to introduce rapidly the newest norms regarding terrorism financing because the ones that were in force were too old or not existing. The two Legislative Decrees, based on the third EU Directive, significantly innovate the existing prevention system in several aspects adjusting Italian norms to the international standards.

[47] Such as the Goldsmith.
[48] EU Directive 2001/96 of December 4th, 2001.
[49] Such as the lawyer, notaries.
[50] Legislative Decree no. 56/04.
[51] EU Directive 2005/60 of October 26th, 2005.

Through the years world trends and technology changed a lot, consequently it was necessary for AML norms to be always updated to keep up with the times. In 2015 the European Parliament enact the IV EU directive[52] that repealed the previous Directive, transposed in Italy in 2017 with the Legislative Decree no. 90. This Legislative Decree unified the previous two Decrees, no. 109 and no. 231, into one law. As we will see later, in chapter no. VI, the fourth EU Directive brought numerous innovations.

In quick succession EU parliament enacted in 2018 the V Directive[53] updating the AML regulation with the assertion of new technology (as virtual currencies) and methods. Italian government transposed the EU fifth Directive in national law with the Legislative Decree no. 125 of October 3, 2019.

2.2. How European and Italian legislations are structured (AML purpose)

As already said in the previous chapter, the European Union started from the first part of the 90's to fight money laundering through a wide production of legislation, thanks to which the European Council tried to regulate a series of specific anti-money laundering obligations. The European Union started to deliberate its obligations through Directives, which are not binding regulations because their recipients are entities who need time to comply with those provisions. The Directives contained the minimum standard that the European countries have to deliberate in their own national law through an internal act. In this way the entities affected by the resolution have two years to comply with the obligations before

[52] EU Directive 2015/849 of May 20th, 2015.
[53] EU Directive 2018/843 of May 30th, 2018.

the Directive can enter into force. The international response to this situation has resulted in an unprecedented level of international cooperation in criminal matters as the nations of the world seek to combat serious crime and the money laundering that inevitably follows[54]. The International cooperation is at the basis of anti-money laundering legislation, sometimes may change quickly because the nature of the phenomena is not stable and it can evolve continuously in the structures. Only through a coordinated cooperation the governments fight against money launders could be effective.

On the National side, the anti-money laundering legislative framework followed the international standards and it has been constantly updated through the years. Nowadays the primary source of AML regulation in Italy is represented by the Legislative Decree no. 231 of November 21st, 2007[55] and by the relative implementing provisions issued by the Ministry for Economy and Finance, by the Financial Intelligence Unit and by the sector supervisory authorities. A cornerstone of the system is the risk-based approach, which should inform the actions of the authorities and the behavior of the obliged entities. Assessing the risks of money laundering and the financing of terrorism make it possible to tailor the measures adopted to tackle them, there by favoring a better allocation of resources[56].

2.3. International and Italian institution

Responding to the money laundering crimes growing awareness, the international community started in the nineties to implement a common strategy

[54] *Responding to Money Laundering International Perspectives*, E. U. Savona, 2005.
[55] Recently amended by the Legislative Decree no. 125 of October 4th, 2019.
[56] Italian Financial Intelligence Unit website, *The National legislative framework*.

through international institution to fight money launders and terrorism financiers. In particular since 1990, international institutions have developed formal processes for imposing sanctions on countries that do not follow the international standards[57]. In the following lines the most important international institutions which have contributed and are still contributing to the fight against money laundering and terrorism financing crimes are described.

The United Nations (UN). The UN were one of the first international organizations that started to take action against money laundering at worldwide level. The law enforcement, organized crime and anti-money laundering Unit of UNODC[58] is responsible for carrying out the global program against money-laundering and the financing of terrorism. It was founded in 1997 in Vienna after the mandate given to UNODC through the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances[59] of 1988 (Vienna Convention). The organization mandate was reinforced in 1998 by the Political Declaration and the measures for countering money-laundering adopted by the General Assembly[60] which extended the aim of the mandate to cover all serious crimes, not only the drug-related offences. The United Nation convened several international summits and developed several programs through the years with the aim to reduce money laundering and terrorism financing activities, as for example the Palermo Convention (*The International Convention Against Transnational Organized Crime,* 2000)[61], the Global Programme against Money Laundering (GPML)[62] and the Security Council Resolution 1373[63]. As described in the United Nation Office on Drugs and Crime presentation "the broad objective of the global program is to strengthen the ability of Member States to implement measures against money-laundering and the financing of terrorism and to assist them in detecting, seizing and confiscating illicit proceeds, as required pursuant

[57] *Crime and Justice,* Vol. 34, M. Levi and P. Reuter, The University of Chicago Press, 2006
[58] United Nations Office on Drugs and Crime (UNODC).
[59] 169 countries are party to the convention.
[60] During its twentieth special session.
[61] Already mentioned in the first chapter.
[62] A research project aimed to increase the international efforts against money laundering crimes sharing new technology, experts and advice to the members of the project.
[63] Resolution adopted on September 28th, 2001 forcing countries to criminalize financing terrorism actions.

to United Nations instruments and other globally accepted standards, by providing relevant and appropriate technical assistance upon request"[64].

The Financial Action Task Force (FATF). The FATF, as aforementioned at the beginning of chapter II, was established in 1989 by the Paris G7 summit with the purpose to encourage an international approach to fight money laundering activities. Nowadays the FATF is composed by 37 countries[65] and works in collaboration with a number of other international institutions. The three anti-money laundering primary functions are:

1. monitoring members' progress in implementing anti-money laundering measures;

2. reviewing and reporting on laundering trends, techniques and counter- measures;

3. promoting the adoption and implementation of FATF anti-money laundering standards globally[66].

In April 1990 the FATF released for the first time *The Forty Recommendations on Money Laundering* report. It is a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction[67]. The Recommendations have been developed in international perspective, they set an international standard which the countries should achieve. Obviously, each country has its own law and regulations so the forty Recommendations are based on principles, which can be flexible depending on the countries' circumstances. The Recommendations have been updated in 1996, in 2003 and lastly in 2012.

The Egmont Group. The Egmont Group is the global institution for the Financial Intelligence Units (FIUs) founded in 1995. The FIUs are independent

[64] UNODC website, *Mandate Presentation*.
[65] FATF website, *Members and Observers*.
[66] *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism*, The International Bank for Reconstruction and Development/The World Bank/ The International Monetary Fund, 2006.
[67] FATF website, *The FATF Recommendations*.

organizations created by national governments that serve as a center for the receipt and analysis of:

1. suspicious transaction reports;

2. other information relevant to money laundering, associated predicate offences and financing of terrorism, and for the dissemination of the results of that analysis[68].

The Financial Intelligence Units are independent and autonomous bodies charged with combating money laundering. Their structure has to be in compliance with the international standards applying to all financial intelligence units (FIUs): they should be operationally autonomous and independently run; they should be the only unit of the kind in the country; they should possess expertise in financial analysis; and they should be able to exchange information directly and independently[69]. These Financial Intelligence Units represent the focus for anti-money laundering national activities. They provide for the exchange of information between financial institution and law enforcement[70]. Whereas some of the money laundering crimes are transnational crimes, the FIUs need to cooperate and collaborate cross-border with the FIUs of other nations. The Egmont Group was established in order to support the national FIUs on their AML initiatives and to promote the exchange of information between Financial Intelligence Units for money laundering and the financing of terrorism cases.

On the Italian side the Legislation points out, in Title I from Article no. 4 and later[71], who are the authorities responsible for carrying out functions aimed to fight and prevent the money laundering and terrorist financing phenomena. Art. no. 4 defines that the Ministry of Economy and Finance is the highest authority, and it is responsible for the anti-money laundering policies to prevent the use of the financial and economic system for the purpose of laundering the proceeds of criminal activities and terrorist financing. In order to implement these policies, the

[68] Egmont Group website, *Financial Intelligence Unit*.

[69] Italian FIU website, *The Role of the Financial Intelligence Unit (FIU)*.

[70] *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism*, The International Bank for Reconstruction and Development/The World Bank/ The International Monetary Fund, 2006.

[71] Of Legislative Decree 231/07 (Last updated on July 16th, 2020).

Ministry of Economy and Finance promotes the collaboration between the Italian FIU, the sector supervisory authorities, professional associations and the police forces, as well as between public and private sector entities. The Ministry also has to manage the relations with the European institutions and international organizations. The Ministry of Finance may avail itself of the *Comitato di Sicurezza Finanziaria*[72] (whose discipline is contained in the Legislative Decree no. 109/07 and later updates) in carrying out its functions of a political - strategic nature. The Committee elaborates the national analysis of money laundering and terrorist financing risks and the strategies to counter it and it also exercises specific powers in terms of fighting the financing of terrorism and the activity of the countries that threaten international peace and security. Another leading organization with an anti-money laundering perspective in Italy is the *Unità di Informazione Finanziaria (UIF)*. It is the Italian Finance Intelligent Unit, already described in The Egmont Group paragraph. The Italian FIU was founded in 2007 with the Legislative decree no. 231, replacing the *UIC*[73] (*Ufficio Italiano Cambi*). The Italian FIU was set up at the Bank of Italy, remaining autonomous and operationally independent[74]. The *UIF* receives and acquires information on money laundering and terrorist financing potential cases mainly through suspicious transactions reports sent by intermediaries, professionals and non-financial operators. The *UIF* conduct also a financial analysis of these data using the sources and powers at its disposal and it evaluates the results for the purposes of transmission to the Special Foreign Exchange Unit of the *Guardia di Finanza* (*NSPV*) and to the Anti-Mafia Investigation Department (*DIA*), which are the competent authorities for investigations[75]. The Italian law also provides the presence of other sectoral supervisory authorities[76], which are in charge to oversee the issuance of regulations in their respective areas of jurisdiction on matters such as customer due diligence, data recording, organization,

[72] The Committee is chaired by the *Direttore Generale del Tesoro* and it is composed by members of the *Ministero dell'Economia e delle Finanze*, *Ministero dell'Interno*, *Ministero della Giustizia*, *Ministero Affari Esteri*, *Banca d'Italia*, *Commissione nazionale per le società e la borsa*, *Istituto per la vigilanza sulle assicurazioni*, *Unità di informazione finanziaria* (FIU), *Guardia di Finanza*, *Direzione investigativa antimafia*, *Arma dei Carabinieri* and *Direzione nazionale antimafia*.

[73] that was turned in an anti-money laundering function in 1991.

[74] Legislative Decree 231/07 (Last updated on July 16th, 2020), Article no. 6.

[75] Italian FIU website, *The National legislative framework.*

[76] Such as the Bank of Italy, *IVASS* and *CONSOB*.

procedures and internal checks[77]. These supervisory authorities also have the power to verify the compliance of their supervised entities with the respective regulations and have the right to exercise power of sanction. The Italian legislative framework, following the international standard, provides also other Governmental institutions, not mentioned before, which are in charge to promote and monitor anti-money laundering obligations to the obliged entities.

2.3.1. International Standard

International standards are principles designed by the international community in order to fight money laundering jointly, with higher effectiveness probability. Nowadays the 2012 revised FATF's 40 Recommendations, already cited in the previous chapter, constitute the international standards for anti-money laundering and for fighting the financing of terrorism. The FATF Recommendations determined the essential measures that countries should have in place in order to:

- "identify the risks, and develop policies and domestic coordination;
- pursue money laundering, terrorist financing and the financing of proliferation;
- apply preventive measures for the financial sector and other designated sectors;
- establish powers and responsibilities for the competent authorities (e.g., investigative, law enforcement and supervisory authorities) and other institutional measures;

[77] Italian FIU website, *The National legislative framework*.

- enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; and

- facilitate international cooperation."[78]

The FATF also issues some guidance and best practices papers with the aim to help the countries and the interested parties to implement their recommendations. The forty Recommendations have been developed with the support of some prestigious international institutions as the World Bank, the International Monetary Fund and the United Nations. In this way all the most important organizations commit to give their contribution to fight a common enemy.

The FATF forty Recommendations were developed following a risk-based approach. The risk-based approach enabled the countries' Governments to implement more flexible set of measures and being more efficient. Thus, they can take a more focused approach on the major risk's areas. To do so, countries must assess and understand the risk of money laundering and terrorism financing to which they are exposed. As explained by the FATF's risk-based approach guidance for the banking sector "when assessing ML/TF[79] risk, countries, competent authorities, and financial institutions should analyse and seek to understand how the ML/TF risks they identify affect them; the risk assessment therefore provides the basis for the risk-sensitive application of AML/CFT[80] measures. The RBA[81] is not a "zero failure" approach; there may be occasions where an institution has taken all reasonable measures to identify and mitigate AML/CFT risks, but it is still used for ML or TF purposes"[82].

[78] *The FATF Recommendation report: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, Financial Action Task Force (Updated October 2020).
[79] Money Laundering/ Terrorism Financing.
[80] Anti-Money Laundering/ Combating Terrorism Financing.
[81] Risk-Based Approach.
[82] *Risk-based approach guidance for the banking sector,* FATF, October 2014.

2.4. Anti-Money Laundering technology and systems

Technology has a crucial role when money laundering is considered. It has given to criminals the opportunity to operate worldwide in an easy manner. They can move high cash quantity through different countries, when they want and no matter where they are. Criminals can transfer large quantity of money to domestic or external accounts easily, ad example using the internet banking[83]. But in the same way technology is also used by whom is in charge to fight money laundering crimes such as public institutions and financial intermediaries. There is a sort of "game" played by criminals and authorities where both try to use technology with the aim to take advantage on the other "player". Criminals are developing new laundering methods based on the most updated technologies, such as through virtual currencies, and the authorities are looking for more efficient approaches in order to prevent and detect money-laundering crimes.

Nowadays thanks to the regulators almost all the organizations that criminals could use to launder money have procedures and systems to prevent laundering and terrorism financing activities. The major players, as banks and some financial intermediaries, needed to implement sophisticated software to comply with the rules. The latest generation of AML software through data and analytics aim to detect faster the unusual activities, monitoring customers and their transactions, lowering at the same time the organizational costs. Moreover, following technology development, some software could be also implemented with artificial intelligence, machine learning and big data analysis. Artificial intelligence has the capacity to identify promptly transaction schemes, behaviors and anomalies giving the staff the opportunity to use better their time focusing on analyzing the results. Furthermore, big data technology allowed organizations to shift from just tracking the financial crime's transactions, to between transactions. Elaborating

[83] *Money Laundering and Terrorist Financing Activities*, F. Milan and A. E. Kurce, Business Expert Press, 2016.

the data collected, organizations can also have a clear understanding of the laundering phenomena and the connected patterns. All this technology allows financial institution to trace with more efficiency the source of the illegal funds and also the person who is trying to launder money. Doing so, through specific systems, the organizations can also share their information with other institution or authorities easily.

2.5. Italian Anti-Money Laundering Legislative Decree

In Italy, as already said, the AML legislative framework consist of the Legislative Decree no. 231/2007 recently amended by Legislative Decree 125/2019, and by the relative implementing provisions issued by the Ministry of Economy and Finance, by the Italian Financial Intelligence Unit and by the sector supervisory authorities. Before moving toward the main focus of this thesis, the Customer Due Diligence, it would be fair to briefly define the national framework which the CDD belong to.

Firstly, it should be specified which entities have to comply with the AML norms; it is expressed in the Article no. 3[84]: obliged entities. The type of organizations which have to comply the norms, changed through the years arriving nowadays to a quite numerous list. These entities are: banking, financial and insurance intermediaries (such as banks, Poste Italiane Spa, SIM, SGR, SICAV, etc.); other financial operators (such as trust, credit brokers, currency exchange operators, etc.); various categories of professional (such as notaries, accountants, lawyers, auditors, etc.); non-financial operators (such as subjects dealing in antiques and art or who acts as intermediary in the trading of such items, professional gold

[84] Legislative Decree no. 231/2007.

traders, providers of virtual currency and digital portfolio services, etc.) and gaming services providers (physical and online, networks and casinos).

Nowadays in the Italian legislative framework we can identify four key pillars:

- Customer Due Diligence obligations;
- Conservation obligations;
- Suspicious transaction reporting obligations;
- Limitation on the use of cash and bearer bonds.

The first key pillar, referred to the CDD obligations, will be widely exposed in the next chapter. Anyway, in this chapter the other key pillars will be presented.

Conservation obligations. Until the fourth EU Directive these obligations were considered as "registration obligations", where all the obliged entities had to register all the operation done above a specific threshold. Where? Italian law made compulsory the establishment of an *AUI* (*Archivio Unico Informatico*) for each obliged entity, where they had to register all the requested operation. In this way, in case of investigation, Italian authorities have the possibility to know all the relevant financial flows. In addition, the law also required a temporary database establishment where all the operations were registered[85], in order to solve the partitioned transaction problem. Doing so the entities have had the capability to intercept also who is trying to avoid the *AUI* detection system through lots of small operations instead of just a bigger one. The fourth EU Directive changed the rules because it shifted the obligations from registration to conservation. Nowadays it is mandatory to conserve also all the customers' data, such as the identity document, the fiscal code and additionally, as example, how many operations over the threshold customers do and all the *registration obligations* of the previous Directive. Bank of Italy suggested to the operators that AUI continues to be the optimal way to comply with the conservation obligations. Doing so, being the entities responsible for the documentation's conservation, the AUI continued to be the main tool for almost all the organizations.

[85] Above a specific threshold determined by the entity.

Suspicious transaction reporting obligations. The Italian regulation requires to the obliged entities to report the suspicious transactions that could be part of money laundering or terrorism financing operations. The report has to be sent to the *UIF* before the operation is done and when the entity knows, suspects or has reasons to suspects that a money laundering or terrorism financing operation is attempted or carried out[86]. To understand if a transaction could be part of money laundering or terrorism financing operations, in order to facilitate the obliged entities, the *UIF* have provided specific red flag indicators and anomaly schemes. As explained by the *UIF* website "the patterns are drawn up based on the experience accumulated in the course of financial analysis and making use of the contribution of the competent investigative and supervisory authorities, and they correlate particular logical and time sequences of facts and behavior that experience shows are traceable to certain criminal activities*".* Some of these anomaly indicators and anomalous behavior patterns and models, as will be also covered later in the thesis, are rather important when the customer due diligence is performed because they can assist the employees to detect potentially dangerous situation. The entities do not need to investigate or search for further information, they have to report according to the function ensured by each organization. The focus of the key pillar is the attention to report only truly suspicious transaction; consequently, before the report goes from the subsidiary or entities office to the *UIF* it needs to be verified from the central AML office (of the entity) that is in charge to settle out second level checks due to their information assets (such as the AUI registration). Italian law underlines the importance about the anonymity of the employee who send the report, required to protect his identity. The *UIF* defines the criteria to verify the reliability of the report once the report has arrived. To verify the reports the *UIF* has the know-how (such as looking at the AUI of all the entities and investigating through multiple database) to choose if they are reliable or not. If the report is not reliable the *UIF* has to notify it to the entity and to archive it but if it is reliable the *UIF* has to transmit it to the police authorities.

[86] Legislative Decree no. 231/2007, Article no. 35.

Limitation on the use of cash and bearer bonds. This is the last key pillar referred to the Italian AML framework. When the first anti-money laundering regulation was approved in 1991 this pillar was the first one and it was considered extremely important, however nowadays it is considered the least important[87] one because of the development of the AML framework with more innovative and effective methods. This pillar does not involve only the obliged entities, as the previous ones, but also the Italian citizens because it requires that all the operation over a specific threshold must be done passing through the financial system. It has been introduced to fight the use of cash, considered one of the common and effective way to launder money due to its non-traceable feature. Passing necessarily through the financial systems, the money laundering transactions have higher possibility to be detected by the authorities due to the numerous obligations that the entities belonging to the financial system have to comply with (such as the customer due diligence and the capability to report suspicious transaction). The Article no. 49[88] has the aim to limit the use of cash and bearer bonds. The threshold for the cash payment has been changed multiple times since 2007 until now and nowadays it is set to EUR 2 000 maximum. It will further change from the January 1st, 2022 decreasing to EUR 1 000 maximum.

[87] Nowadays it is included in the "*further measures*" in the Legislative Decree no. 231/2007.
[88] Of the Legislative Decree no. 231/2007.

CHAPTER III: CUSTOMER DUE DILIGENCE

3.1. What is the Customer Due Diligence?

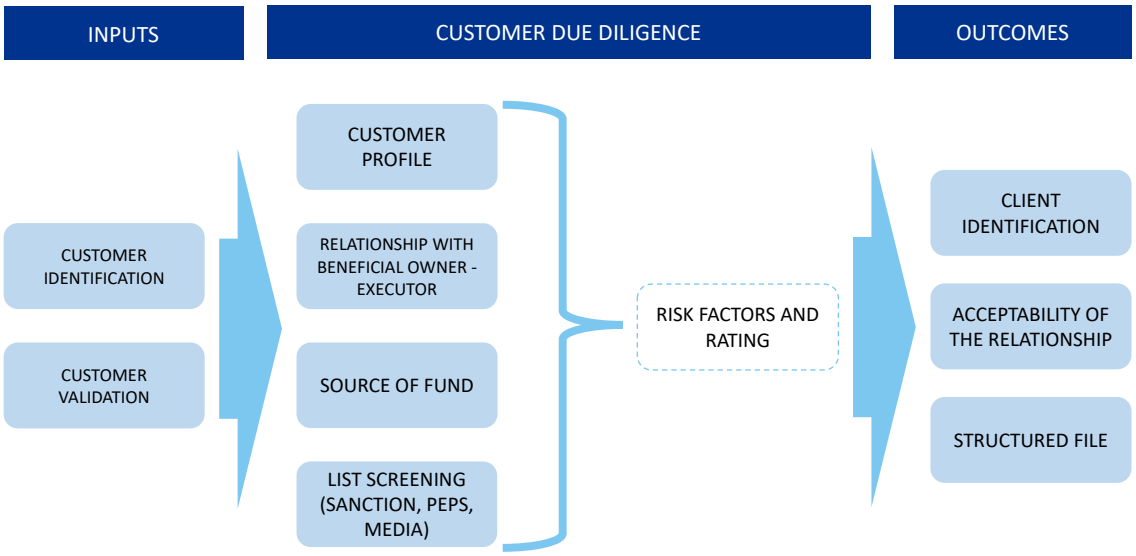
As already mentioned in the previous chapter, the Customer Due Diligence obligation, is one, and probably the most important, pillar of the Italian and European AML legislative framework. The CDD is widely covered in the first Chapter of Title no. II (obligations) of the Legislative Decree no. 231/2007 from Article no. 17 to Article no. 30 and also in Chapter II and III of the EU Directive 2015/849 of the European Parliament and of the Council of May 20th, 2015, recently amended by the EU Directive 2018/843 of the European Parliament and Council of May 30th, 2018.

The CDD obligations are a fundamental and one of the most innovative process of the AML framework. Customer due diligence has been developed with the purpose to limit criminal access to the financial system and to other means of placing proceeds of crime[89]. These obligations are the first and more critical activities that obliged entities have to comply with in order to respect the AML policies, that are developed with the aim to acquire and validate the customer relevant information. The Customer Due Diligence is a process carried out using a number of measures: the identification and checks on the identity of customers and beneficial owners, the acquisition of information on the nature and scope of

[89] *Chasing Dirty Money: The Fight Against Money Laundering*, P. Reuter and E. Truman, 2004.

the relationship and constant checks on the relationship with customers[90]. The following schema (*graph nr. 2*) represent the usual due diligence process.

Graph nr. 2: The customer due diligence process



Source: International Compliance Association

The CDD process begins when a customer requires to establish a business relationship (or some other circumstances that will be covered later on in the chapter) with one of the obligated entities of the AML Decree, and it lasts for their entire relation. The regulators are therefore charging of responsibilities the obliged entities, especially the ones that face more money-laundering risks, adopting the risk-based approach. The CDD process relies on the obliged entity' staff that should obtain their customer information to comply with the regulations; if the staff begin to see financial regulatory requirements as a little more than a regulatory construct, they will not remain as vigilant as should be the case and the money launderer will become a customer[91]. The Customer Due Diligence is the first AML step customers come into contact with. The CDD has been developed a lot through the European Directives; the process, can emphasize the change of mind of the EU legislator, that began from a rule-based approach arriving to a risk-based one. Initially[92] the process was just called "*customer identification*", and it was composed, following the *Know Your Customer (KYC)* principles, by a minimum part of the complex requirement that compose the

[90] Italian FIU website, *The National legislative framework*.
[91] *Handbook of Anti Money Laundering*, D. Cox, Wiley, 2014.
[92] Such as in the first European Directive.

current Customer Due Diligence. The KYC concept was established focusing only on the collection of customer information once the relationship had begun. Otherwise, as we will cover later, the wider concept of CDD includes multiple obligations and it has been developed with strong different methods than the past. It shifted from the simple obligation of customer identification, that nowadays is just the first step, to a more articulated methodology, where sometimes also a customer investigation can be required and a continuous check and monitor of the customer is mandatory. Furthermore, the regulation underline that it is not enough to take only information about the customers, but it is required also, as said before, to analyze in detail the nature and the scope of the relationship. Obliged entities have to constantly evaluate their customers based on their behavior and operation also through the update of their information through the years, with the aim to complete and continuously monitor the customer's profile. If they consider it necessary, entities have also the option to report possible suspicious transactions discovered during the customers profile monitoring, complying with the suspicious transaction reporting obligations described in the previous chapter.

The risk-based approach to CDD was adopted by the FATF as the most effective way to combat money laundering and terrorism financing[93]. The approach requires the adoption of knowing customers process to be proportional to the entity of risks in order to apply the standard, simplified or enhanced due diligence obligations. By definition a risk-based approach cannot define the same procedure for all the scenarios because a standard procedure would be in contrast with the principles of the AML regulation. In Section II, first Chapter of Title no. II, of the Legislative Decree no. 231/2007 from Article no. 23 to Article no. 25 the three CDD types are regulated: standard, simplified or enhanced. The CDD needs to be progressive based on the risk level that different customers have: the intensity and the extent of the CDD requirements should be balanced according to the ML or TF risks level associated with each individual customer [94].

[93] Risk-based Customer Due Diligence, technical notes CGAP, P. Meagher, October 2019.
[94] *Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo*, Bank of Italy, July 30th, 2019.

The risk level needs to be assessed only once the required information during the CDD process are collected. Thus, the customer's risk level definition represents the final phase of the CDD procedure. In case of a low-risk scenario, as in case of a customer being a public authority, some of the CDD requirement can be simplified or excluded. On the other hand, in case of high ML risk scenario, as if the customers are politically exposed person, in order to provide a deeper understanding of the customer activity with the aim to mitigate the risk, CDD obligation requires higher standard and more details.

The risk-based approach defined by the European Directives does not refer only to the three different types of CDD, but as we will cover later, the obliged entities have to assess their exposure level to money laundering and terrorism financing risks in order to define and personalize their internal policies and procedures with the aim of fighting, proportionally to their risk level of exposure, money laundering and terrorism financing. As the money laundering risk level of one business increase, also the CDD procedures will proportionally increase as well. In the obliged entities' anti-money laundering policy, the CDD procedures needs to be properly detailed and the specific types of Due Diligence measures in relation to the different category of customers or products have to be expressed too. Regulation has therefore given to the obliged entities the burden of proof to competent authorities that the implemented policy and measures are appropriate to the risk level they deal with.

Without any doubt the actual CDD obligations have increased the cost and the effort that obliged entities have to invest, if compared to the first Directives obligations, to comply to anti-money laundering norms but institutions are confident that the effort to combat money laundering and terrorism financing are not wasted.

In order to understand deeply the Customer Due Diligence evolution through the European Directives it would be useful to capture the actual scenario, described in the next chapters, defined by the fifth Directive implemented in Italy through the Legislative Decree no. 125 of October 4th, 2019.

3.2. When Customer Due Diligence is needed?

In the fifth European Directive in Article no. 11 and, looking from the Italian perspective in Article no. 17 of the anti-money laundering Legislative Decree, the specific circumstances where the CDD measures have to be applied are defined:

a) "when establishing a business relationship;

b) when carrying out an occasional transaction that:

   i. amounts to EUR 15 000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked[95]; or

   ii. constitutes a transfer of funds, as defined in point (9) of Article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council (1), exceeding EUR 1 000;

c) in the case of persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

d) for providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

[95] Looking to the previous seven days from the first operation date.

e) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;

f) when there are doubts about the veracity or adequacy of previously obtained customer identification data."[96]

These circumstances are the same ones indicated in the FATF Recommendations "*International standards on combating money laundering and the financing of terrorism & proliferation"* updated to October 2020. It is underlined also that obliged entities have to comply with the CDD norms not only to all new customers, but also for the existing ones on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times[97].

3.3. Customer Due Diligence requirements

The CDD requirements are regulated in the fifth European Directive in Article no. 13 and in the Article no. 18 of the anti-money laundering Legislative Decree. The CDD measures can be illustrated as follows.

The obliged entities, in order to comply with the CDD obligations, before the establishment of a business relationship or an occasional transaction execution, have to follow the first authority's indication: the customer and executor's (if it exists) identification. Their identification can be made through ID document if the customer is a natural person, and if it is not, Bank of Italy has provided to obliged

[96] Article no. 11, Directive (Eu) 2018/843 of the European Parliament and of the Council of May 30th, 2018.

[97] FATF Recommendations "*International standards on combating money laundering and the financing of terrorism & proliferation"*, October 2020.

entities a list of criteria to regulate how the identification process works. Therefore, the beneficial owner identification is required as well. The beneficial owner, as will be covered in chapter no. 3.7, “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 and includes at least”[98] some specific circumstances that will be seen in detail later in the thesis. After these steps it is mandatory their identity verification based on their “documents, data or information obtained from a reliable and independent source”. If needed it is also provided the possibility to operate through “remote or electronic identification process regulated, recognized, approved or accepted by the relevant national authorities”. Actually, obliged entities, regardless the type of CDD they decide to execute[99], after the first identification step have at least to collect some selected information on the customer, listed in Article no. 17 of the anti-money laundering Legislative Decree:

“with reference to the customer:

1) the Legal subject;

2) the predominant activity;

3) the behavior demonstrated at the time of the transaction or at the beginning of the business relationship or professional service time;

4) the customer’s or its counterpart’s residence or headquarter area.

With reference to the transaction, business relationship or professional service:

1) the transaction, business relationship or professional service typology to be executed;

[98] Article no. 3, Directive (Eu) 2018/843 of the European Parliament and of the Council of May 30th, 2018.

[99] Standard, simplified or enhanced.

2) the transaction, business relationship or professional service operating methods;

3) the transaction amount;

4) the frequency and volume of the transaction and the length of the business relationship or professional service;

5) the transaction, business relationship or professional service sensibleness in relation to the customer's activity and economic resources in his financial means;

6) the geographical destination area of the product and the subject of the transaction, business relationship or professional service."[100]

The Article no. 22 of the Italian AML Legislative Decree establish that customers must provide in writing and under their responsibility all the necessary information to let the obliged entity to comply with the CDD requirement.

The step further, indicated by the authorities, in order to perform the CDD obligation is the information acquisition on the purpose and on the nature of the business relationship. Entities that perform the CDD have to have a clear understanding of some basic information that can help them to evaluate their customers and their operations. The basic information are the following ones:

1) purpose of the business relationship;

2) relation between customer and executor;

3) relation between customer and beneficial owner;

4) working and economic activity and more in general business relation with the customer.

Thus, obliged entities nowadays cannot limit their DD procedures only to a simple registration of the information received, as it was some years ago, but they must

[100] Article no. 17 of the Legislative Decree no. 231/2007.

have a proactive approach in order to investigate, if necessary, and validate the information received by their customers.

The Italian regulation require also, following the FATF's Recommendations that, in case of ongoing relationship, there must be a continuous customer monitoring. The FATF's recommendation no. 10 specifies that obliged entities "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"[101]. Obliged entities have to keep updated the customer's profile with the aim to detect any incongruence or anomaly that could be considerate in order to comply with other law obligations, such as the suspicious transaction reporting, or the possibility to carry out an enhance due diligence. The ongoing monitoring concept needs to be declared in the entity's AML policy; inside the policy there must be expressed all the measures that employees have to take in order to monitor the customers and also the timing and the frequency of the data updating. Following the already explained risk-based approach, depending on the customer's risk level, the ongoing monitoring can be done with less or high frequency.

In the specific case of relationship, or operation, that involves a third country the obliged entities have the duty to assess the third country's AML system. Doing so the organizations have the capability to understand if a specific country can be defined as a high or low risk one. Bank of Italy provided the obliged entities some documentation that can help them to assess the risk level of each country:

- the reports issued by the International Monetary Fund regarding the *Financial Sector Assessment Programme*;
- the *GAFI* mutual evaluation reports and the high-risk level and not collaborative countries list;

[101] FATF Recommendation "*International standards on combating money laundering and the financing of terrorism & proliferation"* number 10, October 2020.

- the reports approved by the OCSE *Global Forum* on fiscal transparency and exchange of information and the reports on the *Common Reporting Standard*;

- The lists of countries subjected to financial sanctions, embargo and terrorism financing/ proliferation of mass destruction weapons measures.

When entering in a relation with a high-risk country, the European Banking Authority[102] specified that at minimum, following the risk-based approach principles, the obliged entities have to perform the enhanced customer due diligence. To understand if a relationship or transaction involves a third country EBA in the Guideline 4.55[74] published some circumstances where a high risk country is certainly involved: "if the funds were generated in a high risk third country; if the funds are received from a high risk third country; the destination of funds is a high risk country; the firm is dealing with a natural person or legal entity resident or established in a high risk third country; or if the firm is dealing with a trustee established in a high risk third country or with a trust governed under the law of a high risk third country". Furthermore, following the EBA's guideline, the enhanced CDD have to be performed when the transaction passes through a high risk third country, or when a customer's beneficial owner is established in a high risk third country. Obliged entities have also to be careful if at the beginning of a CDD process, their customer or the beneficial owner have personal or professional relation with a high risk third country. Thus, one of the main efforts required to the obliged entities is to evaluate with care, based on the risk level assessed, which DD have to be performed.

[102] In the *Consultation Paper* of February 5th, 2020.

3.4. Customers' risk profile

As aforementioned, the customer due diligence obligation can be performed in three ways: standard, simplified, or enhanced. Obliged entities, following the risk-based approach principles must determine a risk class for each of their customers, and based on the risk class, choose which level of CDD is applicable. To allow organizations to do so, Bank of Italy suggests[103] some sources of information for customer classifications:

- *The Supranational Risk Assessment Report* by the European Commission;
- The report adopted by the *Comitato di sicurezza finanziaria* (AML Decree, Article no. 14 with the "*National risk analysis"*);
- The published report by the investigative and judicial authorities;
- Document provided by the supervisory authorities (such as communication or sanctions);
- Document provided by the *UIF* (such as red flag indicators, anomaly schemes or money laundering cases).

To establish the customers' risk category the process utilizes algorithms and standard computer procedures for increased efficiency and accuracy. The obliged entities usually adopt software that work using computational models which, based on a defined set of information, establish the profile level for each customer. Typically, each entity selects a rating for every criterion that is implemented in the software; thus, when an operational document is registered, the software automatically scores each category. For example, during the ongoing customer monitoring phase, when a cash deposit is made, the customer

[103] Bank of Italy underlined that the information adopted to assess the customer's risk profile can be taken from any documental source and useful document.

must declare the origin of the funds; then, the software provides a rating to the selection: if the origin of the funds is employee income, as a low-risk activity the hypothetical rating equates to 2; however, if the origin of the money is winning at a casino, as a high-risk money laundering activity the hypothetical rating equates to 5. Doing so for each information[104] provided by the customers the software is able to "personalize" the score. Then, the software classifies the customer in the pre-set categories, such as the very high, high, low, or irrelevant. Depending on which category a customer lands in, the standard, enhanced or simplified CDD can be performed. If the software providers are third parties, the entities have to know how the software works and the criteria that are beneficial when determining the customers' risk category. Obliged entities have the ability to amend the customer's risk category from lower to higher, and vice versa; however, should a category change from low to high, the Bank of Italy indicates it is only accepted in exceptional circumstances, with reasons provided in writing.

For each risk category the organizations must define a coherent set of measures in the customer due diligence areas, which goes in an analysis more or less in-depth. Referring to the ongoing relationship each category must have a detailed plan of the customers' profile updates, more frequently in high-risk categories and less often in lower risk categories.

3.5. Simplified Customer Due Diligence

Following the risk-based approach, the Italian AML Decree in Article no. 23, gives the possibility to the obliged entities to apply simplified processes to comply with the customer due diligence obligations. The simplified DD is the lowest level of

[104] Such as the customers' asset, the transaction amount, the type of financial product they acquire, the type of relation between executor and beneficial owner … etc.

due diligence that can be performed on a customer. This is necessary as money laundering and terrorism financing risks are not always the same, with lower-risk circumstances requiring simplified procedures. Obliged entities faced a drain on time and energy, thus introducing the simplified DD, for performing specific customer due diligence for circumstances requiring less effort[105]. The simplified DD differs from the standard one, referring to the reduction of some duties. However, this does not refer to an exemption of the due diligence requirements; the regulation forces the obliged entities to *define and formalize*[106] in detail, in their anti-money laundering policy, the simplified DD procedures.

The Bank of Italy and the AML Decree established a series of circumstances in which the simplified CDD can be performed. They established three types of low-risk categories to help organizations understand if the simplified DD can be performed or not (the Bank of Italy specifies that the list of circumstances is not exhaustive). The first category refers to the customers, executor, and beneficial owner low-risk factors; where the three are considered a low money laundering risk, the simplified DD can be executed. Examples, whereby one of the customer's, executor's, or beneficial owner's low risk factors, may be one of the following: listed companies (with adequate beneficial owner transparency); public administration; customer, executor, or beneficial owner whose residence, or headquarters, or linkages, are located in low-risk geographic areas. The second category refers to the low-risk factors for product, service, operation, or distribution channel, such as: insurance policies (with specific conditions); or welfare systems, in defined cases. The third category refers to the geographic low-risk factors, such as: the European countries; or third countries with efficient AML systems. Nevertheless, the regulation states that the obliged entities must verify permanency of the customers' factors, which allow them to perform the simplified due diligence.

There are circumstances in which the simplified DD cannot be performed; these circumstances are identified when there are doubts about the legitimacy of a

[105] Where there are low risks that a customer became involved in a money laundering or terrorist financing operation.

[106] *Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo*, Bank of Italy; July 30th, 2019.

previously obtained customer's (executor or beneficial owner) identification data; when the circumstances, allowing for the simplified DD to be performed, fail; when the ongoing monitoring identifies a non-low-risk customer (high-risk); or when there are suspicions of money laundering or terrorist financing activity.

So, which are the activities that can be carried out in a simple way?

The Bank of Italy defined multiple measures that obliged entities can choose to adopt:

- "The customer, executor, or beneficial owner's identification document copy may be acquired 30 days from the start of the relationship (for the electronic money instrument the id copy acquisition can be done after the 30 days, but until the instrument activation**);**

- The reduction of some information to be collected, such as the beneficial owner's data, which can be acquired through a customer declaration form (under their responsibility);

- The reduction of the customer's data updating frequency (the data updating can be made in a specific event, such as the opening of a new relationship);

- The reduction of the frequency and depth of the ongoing monitoring analysis (for example, for the ongoing monitoring duty, entities can consider only the operations over a specific threshold)." [107]

Thus, the simplified DD reduces the number of obligations that entities must comply with, aiming to improve the resource allocation to make the customer due diligence system more effective.

[107] *Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo*, Bank of Italy; July 30th, 2019.

3.6. Enhanced Customer Due Diligence

The contrary scenario of simplified DD requires extra identification and ongoing monitoring measures: the enhanced customer due diligence. The enhanced DD is largely performed in situations whereby there is an increased chance of money laundering or terrorism financing through the customer, or the products. The higher level of the CDD is required to mitigate the increased risk; it is regulated by Article no. 24 and 25 of the Italian AML Legislative Decree. A high-risk customer or product does not mean that they are involved in money laundering or terrorism financing activities, however, following the risk-based approach principles, there is an increased chance of involvement in such activities. The obliged entities must perform the enhanced DD when there are specific circumstances provided by the law, or from an internal evaluation.

Correspondingly, for this specific CDD type, the AML Decree and the sector authorities provided a series of circumstances[108] to the obliged entities (divided in three categories), in which it is mandatory to apply the enhanced due diligence. The first category refers to the customers, executor, and beneficial owner's high-risk factors, such as:

- Business relationship, or professional services established under abnormal circumstances;
- Customers that reside or have the headquarters in high money laundering risk geographic areas;
- Economic activities characterized by a high use of cash;
- Structural abnormalities or excessive complexities of customer company's ownership, referring to type of business.

[108] Legislative Decree no. 231/2007, Art. no. 24 and "*Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo"*, Bank of Italy; July 30th, 2019.

The second category defined in the AML Decree is the one that refers to risk factors associated to product, service, operation, or distribution channel, such as:

- Services with high personalization level, offered to high-net-worth individuals;
- Product or operations which may promote anonymity;
- Business relationship, or professional services made remotely, in which the approved identification procedures are not performed;
- Transaction in oil, weaponry, precious metals, tobacco products, and in historical, cultural, or religious goods.

The third category described by the Italian Government regard the geographical risk factor, such as:

- Third countries' AML systems evaluated by reliable and independent sources, and considered ineffective or non-equivalent to the *GAFI* recommendations;
- Third countries that have sanctions, embargoes, or similar measures issued by international authorities;
- Third countries financing terrorist activities.

These are some of the circumstances in which the AML Decree states the enhanced DD must be performed, however, it is not limited to these. The Italian regulation established three scenarios in which it is a requisite for obliged entities to perform the enhanced DD: business relationship or professional services that involve high-risk third countries[109]; cross-border relationship, which include payments with credit or financial institution, based in third countries[110]; or, when

[109] In the *Legislative Decree 231/2007, Article no. 25, comma 4-bis* are listed the duty that obliged entities have to comply with, in order to execute the enhanced DD minimum standards.
[110] In the *Legislative Decree 231/2007, Article no. 25, comma 2* are listed the duty that obliged entities have to comply with, in order to execute the enhanced DD minimum standards.

a Politically Exposed Person (PEP) is involved in a business relationship, professional service or transaction[111].

A Politically Exposed Person is defined by the FATF[112] as "an individual who is or has been entrusted with a prominent public function". The FATF underlines that "due to their position and influence, it is recognized that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering (ML) offences and related predicate offences, including corruption and bribery, as well as conducting activity related to terrorist financing (TF)". As such, due to the high-risk level that PEPs have, the authority's decision to increase the extent and the frequency of the due diligence requirements are justified as a risk-based preventative measure. In case of a PEP enhanced DD, with the intention to go deeper in the investigation, obliged entities should acquire all the information necessary to assess the origin of the PEP's funds. Nowadays, it is the AML Decree that provides the cases in which a person should be considered politically exposed, and the obliged entities must define the procedures to assess if a customer is a PEP or not**.** To do so, obliged entities need to procure the information from reliable sources (such as commercial databases); a specific database for all PEP lists was issued on the Italian authority's website. It is possible that during a business relationship a customer becomes politically exposed, and in this case obliged entities must enhance their due diligence.

The enhanced approach requires obliged entities to perform a deeper analysis, collecting more or superior information on the customer, or beneficial owner, and on the scope and nature of the relationship. Therefore, providing a clearer understanding of the customer and his activities; eliminating the possibility that a money laundering, or terrorism financing operation, is occurring. The in-depth analysis requires a verification and comparison of the data collected, with the intention to obtain evidence; the effort required to perform an enhanced DD is indisputably higher than that of a standard DD: obliged entities are required to develop specific procedures, and organize teams of employees, to ensure timed

[111] In the *Legislative Decree 231/2007, Article no. 25, comma 4* are listed the duty that obliged entities have to comply with, in order to execute the enhanced DD minimum standards.
[112] In the FATF Guidance, *Politically Exposed Persons (recommendations 12 and 22).*

efficiency when investigating a customer, or a transaction. Furthermore, the enhanced CDD rules, following the risk-based approach, include ongoing monitoring, which adheres to increased frequency and higher detail standards, comparatively to the standard one. The overall aim of the specificity is to detect possible ML or TF situations.

3.7. The Beneficial Owner identification

The Beneficial owner is a fundamental element of the current AML regulation. Before entering into the BO' detail it is vital to outline what a beneficial owner is: the fifth EU Directive in Article no. 3 (comma 6) define 'beneficial owner': "it 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…". As will be detailed later the Ultimate Beneficial Owner figure has developed significantly over the years. Currently, the UBO identification is considered a vital element in order to detect possible ML or TF situations.

The purpose of the FATF standards on transparency and beneficial ownership is to prevent the misuse of corporate vehicles for money laundering or terrorist financing[113]. In multiple cases, corporate vehicles, such as companies, trusts, or partnership[114] are used illicitly by criminals as they can hide their identity behind a legal person. The possibility to establish numerous legal person identities, across multiple global jurisdictions, provides criminals the opportunity to keep their real identity hidden; particularly, in countries without transparency laws.

[113] FATF Guidance, *Transparency and Beneficial Ownership.*

[114] Ad example with complex ownership and control structures, hiding the UBOs names.

The regulation aim is to identify the real person/people who have “control” over a company, in a way which could reduce or eliminate anonymity, to identify the true purpose of an account or property, and to identify the source of their funds. Doing so authorities mitigate the risks associated to the beneficial owner.

However, how can obliged entities identify the business relationship, or transactional beneficial owner/s? Legislative Decree 231/2007, following the FATF recommendations, provided in Article no. 20 the criteria to define a legal person’ UBOs (in the case of a natural person, the beneficial owner is the natural person). The law established a series of steps to identify the UBO. The first step identifies a company’s beneficial owner as: the natural person who owns more than 25% of the customer’s capital; or the natural person who owns more than 25% of the customer’s capital through participation of another company. In the circumstances in which the ownership structure doesn’t allow obliged entities to identify the person who owns more that 25% of the capital (some circumstances nobody has a participation higher than 25% of the capital), the law established that the company’s control may be given to: who holds the majority of ordinary shareholders meeting voting rights; who holds enough voting rights to influence the ordinary shareholders meeting; or, who owns specific contractual obligation that allow influence of the ordinary shareholders meeting. Aside from the circumstance in which the customer is a private legal person, the beneficial owner may be identified as the founder, the beneficiaries (if easily identifiable), or they who hold the legal representation, dictionary, or administrative power**.** The law, if the previous criteria cannot be applied, provide a remaining option whereby the UBO is identified as the natural person who is the legal representative, dictionary, or administrative power. Adhering to these criteria, the obliged entities investigate and sometimes request information from the customer, who is obliged to cooperate under their responsibility, more documentation in order to identify, in all the customer due diligence they perform, the beneficial owner. However, some organizational structures are so complex[115] it can require a significant amount of time to complete the investigation, making the CDD a costly effort.

[115] Are based in multiple countries and configurated with very different companies, specifically developed with the aim to hide the beneficial owner identity.

To conclude, the current regulations related to beneficial owner identification are highly structured, highlighting the effort, and importance that international authorities have placed on them during the previous years. In spite of the effort required to the obliged entities to identify the UBOs, sometimes it occurs that criminals try to circumvent the developing rules ad hoc structures. For this reason, the international authorities must maintain their focus on innovating methods to identify the beneficial owner.

3.8. Customer Due Diligence by third parties

The customer due diligence duties can be very costly and require lots of effort. To increase efficiency, the obliged entities have the possibility to "rely on third parties to meet the customer due diligence requirements"[116]. However, if they decide to outsource the CDD process, they will continue to be responsible for the compliance with the CDD requirement, thus obliged entities have to verify the accuracy of the performed DD. If something is wrong, the obliged entity has to inform his third party and, if necessary, modify the report. The Legislative Decree 231/2007, in Article no. 26 lists the third parties that meet the requirement to perform DD for the obliged entities, and from Article no. 27 to no. 30 are covered the third party's due diligence requirements.

The third parties who perform the CDD have to submit, to the entities for whom they work, a report with the information required by law to comply with the customer due diligence norms. The third parties can standardize their due diligence reports developing a specific format for the information collected. To comply with the requirements, based on the different CDD typology they choose

[116] Directive (EU) 2018/843 of the European Parliament and of the Council of May 30th, 2018.

to perform, the third parties collect a series of information that the report should contain[117]: the customer, executor, and beneficial owner identification documents; which sources have been used to verify the customer, executor, and beneficial owner identities; and information on the nature and scope of the business relationship, or occasional transaction, to comply with the CDD specific requirements.

So, through the third parties' support, obliged entities can comply with the ever-increasing CDD obligations without increasing its employees' and operational costs. The third parties that offer CDD services often rely on high-tech solutions and on experienced employees, which allow them to perform CDD requirements most efficiently. Usually, the high-tech solutions are based on complex platforms that are specifically developed for the due diligence execution. The platforms have functions such as the collection of all information available on the internet, in multiple languages, inputting the name, date of birth, and country of the interested subject. These platforms, through artificial intelligence, are able to evaluate some of the results obtained based on the input provided, delivering acutely accurate results, and simplifying the job of the employees.

[117] "*Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo"*, Bank of Italy; July 30th, 2019.

CHAPTER IV: THE FIRST AND SECOND EUROPEAN DIRECTIVES

4.1. The first European Directive

In the previous chapters the actual AML scenario is defined, but how it has developed over the years? As already covered in the Chapter 2.1, the first effort at European level to manage the fight against money laundering has to be identified in the first European Directive. The Council directive 91/308/EEC*,* of June 10th, 1991, on prevention of the use of the financial system for the purpose of money laundering is the first European anti-money laundering Directive. The European Directive has been transposed in Italy with the Legislative Decree no. 143/91[118].

The first time that Customer Due Diligence and its obligations, the main focus of this thesis, was introduced in Europe was in the 1990, when the FATF issued its first 40 recommendations. The FATF issued in the "Customer Identification and Record-keeping Rules*"* chapter the CDD duties that financial institutions have to comply with in order to meet the international standard. Thus, as already said, in 1991 the European Council implemented at European level its first Directive basing on the FATFs' recommendations.

The Directive introduced a European definition of money laundering based on the 1988 Vienna UN Convention (Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances) and called the Member States to prohibit such money

[118] Then amended by the law no. 197 of July 5th, 1991, the first Italian AML legislation.

laundering, at least when it involves the proceeds of drug trafficking[119]. The Directive was the first regulation developed with the aim to fight money laundering with a common and European, strategy. Banks and some others financial institutions are entrusted by the first Directive to play an active role on crimes prevention. The first Directive was only limited to the credit and financial institutions because they were considered to be the most vulnerable to being used by money launderers, even if the directive encouraged the member states also to extend the requirements to money laundering high risky sectors[120].

Basically, the Directive charged some specific financial intermediaries with the financial transaction examination duty. Doing so the regulator aim was to detect possible money laundering transaction and increasing simultaneously the financial market transparency. Furthermore, the Italian law required to the obliged entities the registration of all the transactions record in a specific database, the already covered *AUI* (Archivio Unico Informatico). Following the FATF's recommendation the EU Directive began to implement some customer identification duties, basing on the Know Your Customer (KYC) principles already covered in the chapter 3.1. The Directive required financial institution and insurance companies to identify "the customers by means of supporting evidence when entering into business relations or for any transaction with customers involving a sum amounting to ECU 15 000 or more"[121]. The documents related to the customers identification had to be kept for at least five years after the relationship has ended.

By the way the Directive demanded also to the obliged entities to report suspicious transactions to the competent national authorities. These suspicious transactions sometimes have been difficult to identify because, to be identified as part of a money laundering process, the money must originate from a limited number of crimes: following the Italian penal code to be investigated as money laundering, by the Art. 648-bis and 648-ter, the money source must be related to

[119] *The EU Legislative Framework against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards*, V. Mitsilegas and B. Gilmore, Cambridge University press, 2007.
[120] *Money laundering: A concise guide for all business*, D. Hopton, Taylor & Francis Group, 2009.
[121] Directive (EU) 91/308/EEC of the Council of June 10th, 1991.

aggravated robbery, aggravated extortion, kidnapping or offences relating to the production of or trafficking in substances narcotic or psychotropic. The obliged entities' employees found it difficult to understand if the money source was related to one of the penal code specific crimes or not[122]. Two years after the entry into force of the law, in Italy the suspicious transaction reports submitted to the authorities were just 230[123]. This was due numerous factors involving multiple reasons. One reason is for sure that initially the secrecy of the employee that sent the report was not guaranteed. Thus, the employees did not risk possible dangerous consequences to send the suspicious transaction reports. But being the employees, with their collaboration, one of the pillars of the law, the European Union updated the regulation considering fundamental the secrecy of the employee identity who send the report. Therefore, the European Parliament issued an integration of the Directive with some improvement to the suspicious transaction report process. In Italy the Legislative Decree no. 153 of 26 May 1997 replaced the first Directive suspicious transaction reporting chapter implementing the European requests, such as the reports' sender confidentiality[124].

In Italy the authority responsible for the suspicious transaction report receipt was established as the *Ufficio Italiano Cambi* (*UIC*) [125] and the technical analysis was separate from the investigation activities, conducted by the police forces[126]. However, the Directive did not included any provision regarding the *nature, function and powers* of these authorities[127], so the European countries developed their state's authority with discretion. As a result, there were not a European standard, sometimes resulting in confusing communications when the cooperation between states was necessary. To overcome this problem in 1995, as already said in chapter 2.3, was founded the Egmont Group, the global institution for the Financial Intelligence Units (FIUs). The Egmont Group was

[122] *Normativa Antiriciclaggio e contrasto della criminalità economica,* L. Di Brina and M. L. Picchio Forlati, CEDAM, 2002,

[123] *Le leggi antiriciclaggio,* FABI (Federazione autonoma bancari Italiani) Veneto, 1993.

[124] *La normativa Antiriciclaggio in Italia,* R. Razzante, Giappichelli Editore, 1999.

[125] The responsibility was assigned by the 1997 Legislative Decree no. 153.

[126] *Il controllo pubblico antiriciclaggio in Italia: recenti riforme e prospettive,* M. Pacini, Il Mulino, 2000.

[127] *The EU Legislative Framework against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards*, V. Mitsilegas and B. Gilmore, Cambridge University press, 2007.

responsible for the implementation of a common standard on the Financial Intelligence Unit structure and to promote the exchange of information between FIUs.

In addition to the Directives obligation the Italian transposed Law established a threshold on the cash and bearer bonds transactions over 20 million of Italian Lira[128]. The transactions over that threshold have to be done necessarily through the financial system, having consequently higher possibilities to be detected if there are money laundering suspects. This limitation is the only one of the transposed law that started to affect immediately the obliged entities' customers[129].

To sum up, the Italian law no. 197 targets are identified by Domenico Strammiello[130], as:

- Limitation on the use of cash and bearer bonds;
- customer identification and registration obligations;
- database establishment in all the obliged entities;
- suspicious transaction reporting obligations.[131]

The law provides two different characteristics related to the obliged entities collaboration with the authorities: the active and passive nature of the collaboration. The active collaboration refers to the obliged entities communication to the authorities of information related to the suspicious transactions detected. Whereas the passive collaboration refers to the information collected by the obliged entities and stored in their archives in order to be available to the authorities for their investigation, if needed.

The Directive introduction in the European AML context have introduced a new development that has to be follow by a change in the entities' mentality. The entities now have to trust on the AML regulation in order to fight jointly the money

[128] Article no. 1, Legislative Decree no. 143/91.
[129] *La normativa Antiriciclaggio in Italia,* R. Razzante, Giappichelli Editore, 1999.
[130] Head of treasury sector, Bank of Italy (during the 1993).
[131] *Le leggi antiriciclaggio,* FABI (Federazione autonoma bancari Italiani) Veneto, 1993.

launders. The obliged entities' employees now play a fundamental role in the fight against the money laundering so their training should be carefully considered.

In 1993 an international expert committee chaired by the *GAFI* have visited and evaluated the Italian anti-money laundering system; their conclusion highlights an *appropriate* AML system with some useful guidance for the weakest elements[132]. In addition, the Directive's Article no. 17 provided that the Commission shall prepare a report on the implementation of the Directive and submit it to the European Parliament and to the Council, in order to follow the implementation process. The report "attempts to make a general description and assessment of the way in which the cardinal provisions of this Community text have been implemented as well as to present the work which remains to be done in order to complete and enhance the European anti-money laundering system"[133]. The impact of the first Directive should be considerable due to the fact that it is the first time that a coordination, on money laundering themes, between European countries is needed and it has gone to regulate an area where the regulations where not present in most of the EU countries. The Commission have assessed that the customer identifications Article has been correctly implemented in all member state's countries and the threshold for the identification duties was transposed by some countries with stricter values (in Italy as aforementioned the threshold was established at 20 million LIT, approximately 10700 ECU). The Commission covered that when the report was written the anti-money laundering was considered a criminal offence in the twelve Member countries, instead of the only one before the Directive publication. In conclusion the report underlines that "if matters such as defining the scope of the money laundering offence, the sharing of information with other Member States authorities, legal assistance, and measures concerning seizure and confiscation of criminal proceeds were regulated exclusively at national level without taking into account the necessary coordination and cooperation between the EU Members, such a situation would have a negative impact in the fight against

[132] *Nuova guida agli adempimenti antiriciclaggio e antiusura,* manuale operativo per le banche, gli intermediari finanziari, i sindaci e gli amministratori, C. Ciampi, F. Berghella, G Conforti, U. Fava, E. Granata, C. Lauria, A. Lo Monaco, A. Pansa, Bancaria editrice, 1998.

[133] *First Commission's report on the implementation of the Money Laundering Directive (91/308/EEC) to be submitted to the European Parliament and to the Council*, Commission of the European Communities, COM (95) 54 final, 1995.

money laundering due to the transnational dimension of this phenomenon"[134]. Nowadays the importance that the cooperation between States have, has been developed and encouraged since the time of the first Directive.

4.2. The second European Directive

Actions to fight money laundering have not remained static during the years, the FATF observed that money laundering typologies and trends evolved after their first Recommendation publication. Being the development and promotion of policies to combat money laundering their core purpose, in 1996 the FATF issued their forty Recommendations updating. The Recommendations were revised to take into account the experience gained over the last six years and to reflect the changes which have occurred in the money laundering problem. The main revised Recommendations aim was the extending of the list of predicate offences for money laundering, extending the preventive duties beyond the financial sector, and updating the customer identification system taking into account new technologies[135].

The changes advanced by the FATF in 1996, led the European Commission to start working on a new Directive. Initially the works was delayed significantly by the European Parliament concerns regarding the effect of the duties extended to the legal profession in terms of the right to a fair trial and the principle of lawyer-client confidentiality. After the 9 September 2001 terrorist attack on United States,

[134] *First Commission's report on the implementation of the Money Laundering Directive (91/308/EEC) to be submitted to the European Parliament and to the Council*, Commission of the European Communities, COM (95) 54 final, 1995.

[135] *The EU Legislative Framework against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards*, V. Mitsilegas and B. Gilmore, Cambridge University press, 2007.

the authority's investigations reveled the money laundering network that al Qaeda used in order to finance itself. The al Qaeda attack highlighted the serious challenges that law enforcement authorities face. On October 30th, 2001 at an emergency meeting, FATF President Clarie Lo announced that "our mission is to strangle and cut the supply of money and assets that is the lifeblood of terrorists"[136]. The FATF, under the members' mandate, added on its mission the development of standards in the fight against terrorist financing. Therefore, the FATF issued its first eight special Recommendations to deal with the issue of terrorist financing. As a result, the European Parliament, feeling the urgency to issue a new Directive to keep up with the times, reached a compromise and the December 4th, 2001 amended the Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering with the Directive 2001/97/EC of the European Parliament and of the Council. The European Directive has been transposed in Italy with the Legislative Decree no. 56 of February 20th, 2004.

The second Directive has innovated some aspect of the previous one. Firstly, the Directive extended the money laundering predicate offences; initially it involved only the proceeds of drug trafficking or little more but in the second Directive was included, as money laundering predicated offences, all the "serious crimes" such as organized crime, corruption, fraud and also drug trafficking as well. The Directive did not limit the predicate offences only to specific crimes as was done in the first one, the EU Parliament understood that money launders can develop and change their methodologies very fast in order to avoid the states' laws. As a result, the Directive indicate as "serious crime" "an offence which may generate substantial proceeds and which is punishable by a severe sentence of imprisonment in accordance with the penal law of the Member State"[137]. Doing so the EU Parliament has extended the money laundering predicate offences from narcotic criminals only to a wider range of offenders.

[136] *The International Lawyer, the impact of September 11 on Anti-Money Laundering Efforts, and the European Union and Commonwealth Gatekeeper Initiatives,* N. M. Healy, 2002.
[137] Directive (EU) 2001/97/EC of the European Parliament and of the Council of December 4th, 2001.

At this stage the EU regulators, with the Member States' support, are evaluating which type of entities should be considered to be obliged to the Directive's duties. The regulators decided, in the second Directive, to provide a list of specific profession instead of leaves to the Member States the possibility to extend the obligation, as done in the first one. Following Betti (2001) "the efforts to update the 1991 directive start from the assumption that an effective fight against money laundering cannot limit itself to involving the cooperation only of credit and financial institutions. A number of other non-financial professions vulnerable to money laundering are identified, as it is acknowledged that 'the tightening of controls in the financial sector has prompted money launderers to seek alternative methods for concealing the origin of the proceeds from crime'"[138]. The discussion of the European Parliament was focused on the identification of the businesses which can be classified at money laundering risk, in a way that these entities can identify properly their customers. At the end the Parliament has even expanded the entities' list initially proposed by the EU Commission. With the development of the anti-money laundering framework the regulators' focus switched from who should be obliged, to how the identification process and the obligations should work.

The second EU Directive impose to Member States to obligate, with the Directive's duty, the riskier businesses identified as the ones which are characterized by high cash quantity handling or the ones through which high value businesses are possible (such as real estate, precious metal, etc.). The EU Parliament classified the following entities:

1. "credit institutions;

2. financial institutions.

And on the following legal or natural persons acting in the exercise of their professional activities:

3. auditors, external accountants and tax advisors;

[138] *The European Union and the United Nations Convention against Transnational Organized Crime*, working paper, S. Betti, European Parliament, 2001.

4. real estate agents;

5. notaries and other independent legal professionals, when they participate in a series of specific financial activities[139];

6. dealers in high-value goods, such as precious stones or metals, or works of art, auctioneers, whenever payment is made in cash, and in an amount of EUR 15 000 or more;

7. casinos."[140]

Following Mitsilegas and Gilmore (2007) the Directive, in order to overcome the confidential nature of lawyer-client relationship problem, "provides the possibility to Member State of exempting lawyers on a number of occasions from the duties of suspicious transaction reporting and (not) tipping off"[141]. In other words the Directive underlines that Member State shall not be obliged to implement in their transposal, the exemption or not in specific circumstances "to notaries, independent legal professionals, auditors, external accountants and tax advisors with regard to information they receive from or obtain on one of their clients, in the course of ascertaining the legal position for their client or performing their task of defending or representing that client in, or concerning judicial proceedings, including advice on instituting or avoiding proceedings, whether such information is received or obtained before, during or after such proceedings"[142]. The Italian transpose law established the suspicious transactions reporting obligation exception to the auditors, external accountants, tax advisors, notaries and independent legal professionals in specific circumstances described in Article no. 2, comma 3 of the Legislative Decree no. 56 of February 20th, 2004.

---

[139] Such as buying and selling of real property or business entities; managing of client money, securities or other assets; opening or management of bank, savings or securities accounts and others. See Article no. 2a.

[140] Article nr. 2a, Directive (EU) 2001/97/EC of the European Parliament and of the Council of December 4th, 2001.

[141] *The EU Legislative Framework against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards*, V. Mitsilegas and B. Gilmore, Cambridge University press, 2007.

[142] Directive (EU) 2001/97/EC of the European Parliament and of the Council of December 4th, 2001.

The European legislator wanted to entrust some professional categories with an authority's supporting functions helping them to identify anti-money laundering operations or money launderers. The legislator attempted also to "prevent clients from using the services of lawyers and notaries to launder the proceeds of criminal activities, or otherwise concealing or disguising the source of funds or other property, in connection with criminal activity"[143].

As aforementioned the second EU Directive, with reference to the customer due diligence, was issued following the 1996 FATF Recommendations. The Recommendations were developed, as the ones in 1990, in accordance with the Know Your Customer principles. Thus, in the first two Directives there are not huge innovation as would be in the third one. The second Directive major impacts on the customer due diligence procedures may be define as follows.

Firstly, the Directive duties are extended to a higher number of obliged entities. Of course, the customer due diligence procedures are extended too. Having extended the CDD procedures to a wider range of professions the Legislator aim was to record the highest number of customers identified, in order to investigate better on the money laundering transactions. Moreover, also the new obliged entities must comply with suspicious transaction report duty. Their contribution should help the police authorities in order to detect more money launders as possible. Of course, the new obligations can be costly for some entities, but the regulator believe that their support could be useful in the common fight against money laundering. Another novelty in the second Directive CDD Article is the one that regard the casinos. The Directive force casinos' managers to identify all their customers "if they purchase or sell gambling chips with a value of EUR 1 000 or more"[144]. The Directive establish also, for the casinos subject to State supervision, the identification and registration of all their customers "immediately on entry, regardless of the number of gambling chips purchased"[145]. These obligation were developed in order to fight the money laundering transactions

[143] *The International Lawyer, the impact of September 11 on Anti-Money Laundering Efforts, and the European Union and Commonwealth Gatekeeper Initiatives,* N. M. Healy, 2002.

[144] Article no. 3, Comma 5, Directive (EU) 2001/97/EC of the European Parliament and of the Council of December 4th, 2001.

[145] Article no. 3, Comma 6, Directive (EU) 2001/97/EC of the European Parliament and of the Council of December 4th, 2001.

made through the casinos. The money launders can enter to the casino with dirty money and change it with casino's chips*,* after that the chips can be re-changed with money that seems lawful. The last customer due diligence Directive novelty regard the "non-face-to-face" operations. The Directive underlines that "establishing business relations or entering into a transaction" with a customer who is not physically present for identification purposes, have higher risk of money laundering. Thus, the Directive asks to Member States to "ensure that the institutions and persons subject to this Directive take specific and adequate measures necessary to compensate the greater risk of money laundering"[146]. The obliged entities, when a customer is not physically present, have to validate the customer's identity requiring "additional documentary evidence, or supplementary measures to verify or certify the documents supplied, or confirmatory certification by an institution subject to this Directive, or by requiring that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution subject to this Directive"[147]. Furthermore, the obliged entities have to write down in their internal policies the measures they propose to take in order to reduce the non-face-to-face money laundering risk. These Directive's non-face-to-face obligations have in a certain way anticipated the problem that the EU Legislator faced years later due to the technology development.

The KYC procedures for the obliged entities are extremely important because if they don't implement the duty requested, they could face serious risks. As the Basel Committee on Banking Supervision "the inadequacy or absence of KYC standards can subject banks to serious customer and counterparty risks, especially reputational, operational, legal and concentration risks"[148]. These risks have to be managed by the entities in order to prevent sanctions or increase costs to solve and mitigate the problems faced. Thus, having adequate KYC procedure

[146] Article no. 3, Comma 11, Directive (EU) 2001/97/EC of the European Parliament and of the Council of December 4th, 2001.

[147] Article no. 3, Comma 11, Directive (EU) 2001/97/EC of the European Parliament and of the Council of December 4th, 2001.

[148] *Customer due diligence for banks,* Basel Committee on Banking Supervision, Working Group on Cross-border Banking, Bank for International settlements, October 2001.

is fundamental to comply with the regulations and to avoid the risks covered by the Basel Committee on Banking Supervision.

4.3. The rule-based approach

Both the first and the second EU Directives, as stated above, have been developed basing on the FATF forty Recommendations. These Recommendations, published respectively in 1990 and in 1996, were established focusing on a rule-based approach. These rule-based approach regulations provide to the obliged entities clear legal provision which have to be respected, the approach aim is the duty to act following the rules imposed by the regulator. The characters of the rule-based approach can be defined as follows:

- "relevant measures or behaviors are pre-determined by rules;
- given the same "triggering events" (e.g. transactions over a threshold), the same behaviors apply in all situations;
- compliance is achieved when pre-determined behaviors are adopted, regardless of their suitability ("formal" component);
- no or little discretion in adapting the measures to the concrete case (equal treatment of different situations)."[149]

The rule-based can be identified as a "static" approach, where the obliged entities have just to follow the rules to be compliant with the norms. The regulators set

[149] *Rule-Based vs. Risk-Based approaches to control. The third EU AML/CFT Directive Conference,* Utrecht School of Economics, P. Costanzo, European Commission, November 2007.

the criteria for the identification of possible money laundering circumstances[150] and obliged entities must follow it. No proactive attitude is requested and within a dynamic and evolving environment, as money laundering is, the rigidity of the system sometimes cannot result in a best effort.

Following Costanzo (2007), the rule-based approach pros are the certainty of the "situations" (such as the equal treatment of different situations with no or little discretion), the easy compliance achievement and the easy controls that entities could perform. The approach does not require high specialized employee in order to carry out the check demanded by the norms because most of their job is standardize on the bases of the procedures and norms. These rule-based approach "standardizations" should be implemented by the Legislators, that provides to obliged entities a series of measures that have to be followed in order to apply the norms, without giving space for any interpretation.

In conclusion following the B. Unger and F. Van Waarden study "the rule-based approach led to over-reporting, as many of the reported transactions had nothing to do with money laundering, but at least there were clear criteria about what to report and it was easy for the government to control this reporting and to impose fines on banks that did not report according to these criteria"[151].

[150] Such as all the transaction made over a set threshold must be considered suspect and reported.

[151] *Review of Law & Economics: How to Dodge Drowning Data? Rule- and Risk- Based Anti-Money Laundering Policies Compared,* B. Unger and F. Van Waarden, Utrecht University School of Economics, Bepress, 2009.

CHAPTER V: THE THIRD EUROPEAN DIRECTIVE

As previously disclosed, the second EU Directive was issued in 2001 and enforced in Italy in 2004. The Directive was updated to follow the 1996 FATF's Recommendations aiming to increase response time to the external environment to which the Directive adheres; the same happened for the third EU Directive. To begin, I will present the chain of events leading to the publication of the third EU Directive.

In June 2003 the FATF issued the updated Forty Recommendations, to involve the terrorism financing provisions, following the 2001 mandate extension. As presented by the FATF in its 2003 Recommendations introduction: "the revised Forty Recommendations now apply not only to money laundering but also to terrorist financing, and when combined with the Eight Special Recommendations on Terrorist Financing provide an enhanced, comprehensive and consistent framework of measures for combating money laundering and terrorist financing"[152]. The terrorist attacks that were happening highlighted the lack of preparation on behalf of the State and European laws, which were aimed at preventing such attacks. Money laundering and terrorism financing must be combated with an international, collective strategy; single measures adopted at national level, without taking into consideration the international cooperation needed, will achieve an inadequate effect, and cam be constituted time-consuming, and wasted efforts. Thus, the European Legislator feels the Member States pressure to align its regulations with an International standard, even if they are not legally binding.

The aforementioned reasons express the EU legislator prioritizing the third Directive, thus, October 26th, 2005, issued the Directive of the European

[152] *The Forty Recommendations,* Financial Action Task Force on Money Laundering, June 20th, 2003.

Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, and terrorist financing. For the first time the Directive title included the supplement “terrorism financing”, in order to underline its role in combating the terrorism financing framework.

Following Fernandez Salas (2005), the European Parliament and the Council were aware of the importance of publication of the Directive, as reflected in the speed of the legislative procedure; “it has taken less than 12 months since the presentation of the Commission proposal to reach an agreement on a text”[153].

The third EU Directive was transposed in Italy in two Legislative Decrees. Firstly, the Italian Government transposed the section of the Directive referring to the prevention of terrorist financing, with the Legislative Decree no. 109, June 22nd, 2007, as the regulations referencing combatting terrorist financing were non-existent or, outdated. Secondly, the Italian Government transposed the Anti-money laundering section with the Legislative Decree no. 231 of November 21st, 2007.

5.1. The Third Directive structure and the 2003 FATF Recommendations

The Third EU Directive was published repealing the previous one. As the second Directive amended the original Directive, the Commission considered a rewrite necessary due to the numerous modifications. At first glance the third Directive is more structured and more specific than the previous two, due to the accumulated

[153] *The third anti-money laundering directive and the legal profession*, M. Fernández Salas, October 2005.

experience. It is divided in the following seven chapters, which are subdivided into Sections and Articles:

1. Subject-matter, scope and definitions;
2. Customer due diligence;
3. Reporting obligations;
4. Record keeping and statistical data;
5. Enforcement measures;
6. Implementing measures;
7. Final provisions.

As aforementioned, the Directive was issued with a focus on the international standards adopted in 2003 by the FATF (the forty Special Recommendations), and on the further eight Special Recommendations, aimed at combatting terrorist financing, implemented in October 2001[154]; which, when combined with the FATF Forty Recommendations, outlined the basic framework to detect, prevent, and suppress the financing of terrorism (the ninth special Recommendation text was not integrated in the Forty Recommendations). The 2003 FATF Recommendations structure was revised entirely compared to the previous Recommendations. The revised structure was divided into four sections:

A. "Legal system (Recommendations 1 to 3);
B. Measures to be taken by Financial Institutions and Non-Financial Businesses and Professions to prevent money laundering and terrorism financing (Recommendations 4 to 25);
C. Institutional and other measures necessary in system for combating money-laundering and terrorist-financing (Recommendations 26 to 34);

[154] In October 2004 was issued a ninth Recommendations.

D. International co-operation (Recommendations 35 to 40)."[155]

At the end of the text there is a Glossary and Interpretative Notes on the Forty Recommendations.

The Forty Recommendations amendment was implemented in all sections of the text. One major change was made in Recommendations no. 1: the FATF developed the 1996 First Recommendation, expanding money laundering predicate offences to all the "serious offences", replacing it with a new text: "countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences"[156]. Thus, resulting in the FATF encouraging members to increase the number of crimes considered predicate offences for money-laundering related crime.

The Recommendations relevant to this thesis are almost exclusively found in section B, from 5 to 12[157]. FATF's Recommendations established a series of circumstances in which obliged entities have the duty to perform the CDD and these circumstances are the same of the third EU Directive, which we will cover later. The CDD duties that obliged entities, following the FATF, have to undertake are the following:

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 taking reasonable measures to understand the ownership and control structure of the customer;

[155] *The Forty Recommendations,* Financial Action Task Force on Money Laundering, June 20th, 2003.
[156] Recommendation no. 1, *The Forty Recommendations,* Financial Action Task Force on Money Laundering, June 20th, 2003.
[157] *Customer due diligence and record-keeping* chapter.

c) 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."[158]

The key innovation on CDD themes introduced by the 2003 FATF Recommendations is the risk-based approach. Until 2003 the FATF guidance and the EU Directives adopted a rule-based approach (already covered in chapter 4.3). This risk-based approach has been an innovative, enduring enforcement, following Gilmore (2011) "by adopting a risk-based approach, it is possible to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greater risks receive the highest attention. The alternative approaches are that resources are either applied evenly, or that resources are targeted, but on the basis of factors other than risk. This can inadvertently lead to a "tick-box" approach with the focus on meeting regulatory requirements rather than on combating money laundering or terrorist financing efficiently and effectively"[159]. The obliged entities have to assess their customer's risk level and perform the CDD accordingly. Following Recommendation 5, obliged entities "may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction"[160]. Moreover, for the first time the FATF introduced three different customer due diligence types: enhanced, simplified, or standard; performed dependent on the customer's assessed risk level. The Forty Recommendations,

[158] Recommendation no. 5, *The Forty Recommendations,* Financial Action Task Force on Money Laundering, June 20th, 2003.

[159] *RBS Guidance for Legal Professions*, Paris, FATF, October 23rd, 2008; *Dirty Money, the evolution of international measures to counter money laundering and the financing of terrorism*, W. C. Gilmore, Council of Europe Publishing, October 2011.

[160] Recommendation no. 5, *The Forty Recommendations,* Financial Action Task Force on Money Laundering, June 20th, 2003.

2003, identified specific high-risk areas, such as the politically exposed persons, and relating to cross-border correspondent banking and other such relationships, in which a series of definite measures must be executed (respectively Recommendations 6 and 7).

To conclude, Section C (institutional and other necessary systematic measures for combating money laundering and terrorist financing) of FATF's Recommendations, 2003, has undergone significant developments too. As specified by Gilmore (2011), FATF Recommendations, 1996, in part failed to consider the establishment of the Financial Intelligence Unit[161]. Nevertheless, Recommendation 26, 2003, was intended to fill the gap, and as such, it required to its Members to implement specific core competences to their Financial Intelligence Units; the FIUs have to work "as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of STR and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR"[162].

5.2. The Third Directive Scope and Definitions

The third Directive established a more succinct definition of money laundering, and terrorism financing. For the first time the Directive asked the Member States

[161] *Dirty Money, the evolution of international measures to counter money laundering and the financing of terrorism*, W. C. Gilmore, Council of Europe Publishing, October 2011.
[162] Recommendation no. 26, *The Forty Recommendations,* Financial Action Task Force on Money Laundering, June 20th, 2003.

to prohibit *in toto* money laundering, and terrorism financing[163]. The money laundering definition is as stated in chapter 1.1[164], demonstrating the maturity and experience reached by the EU legislator on money laundering themes. Following Mitsilegas and Gilmore (2007), the money laundering definition was amended to align the "serious crime" Directive's definition with the one included in the 2001 Framework Decision on confiscation[165]: what constitutes a "serious crime" are all the offences **"**which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards those States which have a minimum threshold for offences in their legal system, offences punishable by deprivation of liberty or a detention order for a minimum of more than six months"[166].

Though, Terrorist Financing in the third Directive "means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of June 13th, 2002 on combating terrorism" [167]. This Council Decision on combating terrorism, June 13th, 2002, defined a terrorist group and listed three categories of terrorist related crime: "terrorist acts against fundamental rights and principles, offences connected with terrorist groups, and offences connected with terrorist activities" [168].

Further in the chapter, will be discussed the following in more depth: the introduction of the "beneficial owner" and "politically exposed person" concepts. Moreover, comparatively to the previous two Directives, the third Directive

[163] In the previous two Directives money laundering was prohibited only as defined in the Directives.

[164] The one included in the V EU Directive.

[165] T*he EU Legislative Framework against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards*, V. Mitsilegas and B. Gilmore, Cambridge University press, 2007.

[166] Article no. 1, comma b, Council *Framework Decision on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime*, 2001/500/JHA, of June 26th, 2001.

[167] Article no. 1, comma 4, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.

[168] *Legislation of the European Union, The Third EU Directive on Money Laundering and Terrorist Financing*, Volume XIII, J. Vyhnálik and I. Fendeková, National Bank of Slovakia, September 2005.

extended the obliged entities list to a broader group. In the Directive, the EU Legislator chose to apply the obligations to "trust or company service providers,"[169] and to all the "other natural or legal person (not mentioned in the obliged entities list) trading in goods, only to the extent that payments are made in cash in an amount of EUR 15 000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked"[170].

As previously stated, the third EU Directive, introduced the term of the Beneficial Owner. The introduction of the BO was necessary to "prevent the misuse of corporate vehicles for money laundering or terrorist financing"[171]. In a dynamic environment, in which the money launderers rapidly evolve their methodologies, by frequently operating corporate vehicles, the Regulator attempted to reduce the scope of their action by establishing stricter measures. The following chapter will cover the circumstances in which obliged entities must perform the BO identification. Next, we will outline the Beneficial Owner definition. The Directive defined the BO and provided two specific circumstances: corporate entities and legal entities. Following Article no. 3, comma 6 "'beneficial owner' means the natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted. The beneficial owner shall at least include:

a) in the case of corporate entities:

    i. the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; a percentage

[169] Article no. 2, comma 3 c, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.
[170] Article no. 2, comma 3 e, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.
[171] FATF Guidance, *Transparency and Beneficial Ownership.*

of 25 % plus one share shall be deemed sufficient to meet this criterion;

ii. the natural person(s) who otherwise exercises control over the management of a legal entity;

b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:

i. where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 25 % or more of the property of a legal arrangement or entity;

ii. where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;

iii. the natural person(s) who exercises control over 25 % or more of the property of a legal arrangement or entity."[172]

The Directive established precise criteria to aid obliged entities assessment of their customers' BO in order to perform the mandatory duties.

Another major revision of the third EU Directive is the concept of the politically exposed person. As outlined for the BO, this chapter will outline the Directive's PEP definition; in the next chapter we will cover in depth the PEP related procedures. The Directive Article no. 3 specifies the PEP definition, following the EU Legislator a "'politically exposed person' means natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons"[173]. There will be a clear evolution of this definition in the next two Directives, conveying the ever-developmental challenges faced by anti-money launderers.

[172] Article no. 3, comma 6, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.
[173] Article no. 3, comma 8, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.

5.3. Obligations related to customer due diligence procedures

During the first two European Directives the Legislator was focused on identifying which obliged entities should perform the CDD duties. The anti-money laundering discipline development during the years, pushed the European Union to focus on how to identify the customers instead of understanding who should perform the duties. The first amended Directive imposed the CDD duties but gave the obliged entities little specification on the procedures that they have to implement. In the third Directive the European Parliament in order to adopt the new international standards and with the aim to develop the anti-money laundering framework, published "more specific and detailed provision relating to the identification and verification of the customer and of any beneficial owner"[174]. The Customer Due Diligence section is number 2 of the Directive and is composed of 13 Articles (Article no. 6 to 19 of the Directive).

5.3.1. When Customer Due Diligence is needed?

Article no. 7 established a series of criteria with the aim to provide obliged entities with specific circumstances that should be considered in order to apply the CDD duties: "the institutions and persons covered by this Directive shall apply customer due diligence measures in the following cases:

[174] *The third anti-money laundering directive and the legal profession*, M. Fernández Salas, October 2005.

a) when establishing a business relationship;

b) when carrying out occasional transactions amounting to EUR 15 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

c) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;

d) when there are doubts about the veracity or adequacy of previously obtained customer identification data."[175]

What is considered a "business relationship" for the EU Legislator is defined in the Article no. 3 of the Directive: "'business relationship' means a business, professional or commercial relationship which is connected with the professional activities of the institutions and persons covered by this Directive and which is expected, at the time when the contact is established, to have an element of duration"[176].

These circumstances will be amended carefully in the next Directives in order to update the regulation and establish even more accurate conditions to assist obliged entities to comply with their duties.

5.3.2. Customer Due Diligence requirements

The third Directive's CDD requirements are regulated in Article no. 8. The third Directive provides the obliged entities with specific procedures that must be

[175] Article no. 7, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.

[176] Article no. 3, comma 9, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.

applied, and moreover it has extended the procedures compared to the previous two Directives.

Following the Directive, the CDD procedure are substantially the following:

a) “identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

b) identifying, where applicable, the beneficial owner and taking risk-based and adequate measures to verify his identity so that the institution or person covered by this Directive is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer;

c) obtaining information on the purpose and intended nature of the business relationship;

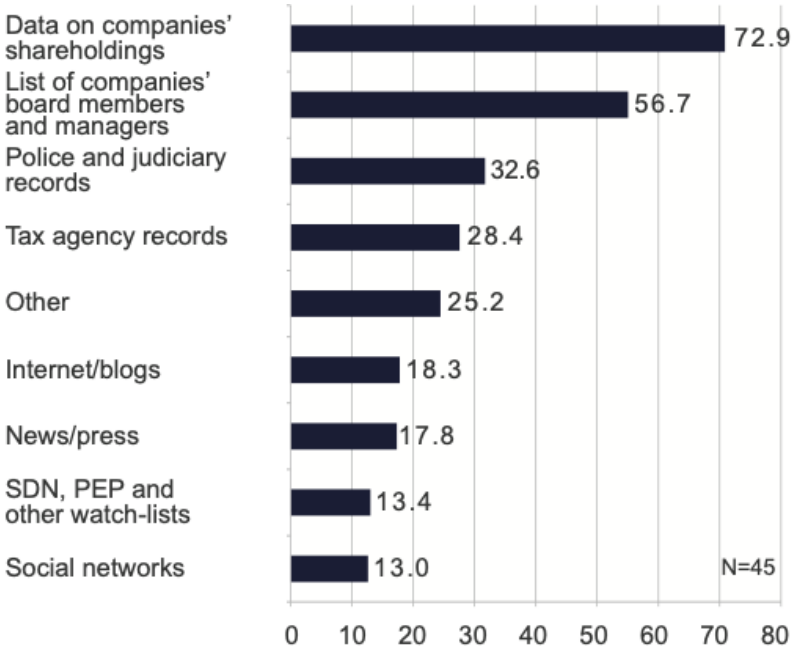
d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's or person's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.”[177]

As mentioned earlier in the thesis one of the major innovations introduced in the third Directive is the customer due diligence risk-based approach. The measures can be “personalized” on the basis of the customer’s risk assessed. The obliged entities, before beginning the CDD procedures, have to “determine the extent of such measures on risk-sensitive basis depending on the type of customer, business relationship, product or transaction”[178]. As regulated by the Directive,

[177] Article no. 8, comma 1, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.
[178] Article no. 8, comma 2, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.

the know Your Customer principles used in the past have been overcome. It is no longer necessary only the general gathering of information regarding customers, but with the new Directive obliged entities have to make a step further in order to assess the customer's risk level and choose how much in-depth the customer's identification should go. The Directive introduced also the beneficial owner identification duty. The BO identification was imposed with the aim to reduce the money laundering processes that involve corporate entities. Following Fernández Salas (2005) "identifying a beneficial owner is not always easy. This difficulty is especially higher in the case of legal entities, such as foundations, and arrangements, such as trusts"[179]. Thus, how can the obliged entities identify properly the ownership and the control structure of companies? A European survey, conducted by the BOWNET project, among the competent authorities highlighted that the "information most frequent used to reconstruct the ownership structure (OS) and the BO of suspicious corporate entities consist of data on company shareholders followed by information on board members and managers"[180] (as reported in the graph no. 3).

Graph nr. 3: What data/information do you use to reconstruct the OS and identify the BO of suspicious corporate entities?



Source: BOWNET survey on EU competent authorities

[179] *The third anti-money laundering directive and the legal profession*, M. Fernández Salas, October 2005.

[180] *The identification of beneficial owner* of legal entities *in the fight against money laundering,* Final Report of Project BOWNET, 2013.

Obliged entities, in order to comply with the third Directive, have to develop their offices and their employees in such a way they can proactively investigate and elaborate the information collected with the aim to identify suspicious customers.

The obliged entities' responsibility has grown a lot with this Directive's duty, because the extent of the CDD procedures is now definite by the entity itself. Moreover, they have to be able to "demonstrate to the competent authorities … that the extent of the measures is appropriate in view of the risks of money laundering and terrorism financing"[181].

Following the casinos' Article no. 10, the Directive increased the quantity of cash spent regarding the customers' identification duty. In the previous Directive the customers who "purchase or sell gambling chips with a value of EUR 1 000 or more"[182] had to be identified, but in the third Directive the Legislator raised the limit to a value of EUR 2 000, if their customers "purchase or exchange gambling chips"[183].

The Directive established for the first time, following the risk-based approach principles, three types of different CDD: standard, enhanced and simplified. Chapter 3.5 of the thesis has already covered in-depth the actual simplified CDD scenario. The one established in 2005 was less defined and less accurate than the one in force now. The third Directive issued the circumstances in which the simplified DD was permitted, and following the Directive's Article no. 11 they were just a few: (a) when the customers is a credit or financial institution covered by this Directive, or a credit or financial institution situated in a third country which imposes requirements equivalent to those laid down in this Directive and supervised for compliance with those requirements; (b) when the customers is a company listed; (c) when the beneficial owners of pooled accounts are held by

[181] Article no. 8, comma 2, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.

[182] Article no. 3, Comma 5, Directive (EU) 2001/97/EC of the European Parliament and of the Council of December 4th, 2001.

[183] Article no. 10, comma 1, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.

notaries and other independent legal professionals from the Member States; and (d) when the customer is a domestic public authority[184].

The Directive has established specific duty for the enhanced due diligence too. Following the EU Legislator, the enhanced DD have to be performed "in situations which by their nature can present a higher risk of money laundering or terrorist financing, and at least in the situations set out in paragraphs 2, 3, 4 and in other situations representing a high risk of money laundering or terrorist financing which meet the technical criteria established in accordance with Article 40(1)(c)"[185]. Those situations which can present higher risk of ML or TF are the ones where: the customer is not physically present for the identification procedures (non-face-to-face-operations); there are banking relationship with cross-frontier institutions from third countries; or, when a politically exposed person "residing in another Member State or in a third country"[186] is involved. For each of the situations covered in the previous lines the EU Legislator issued a series of specific measures that obliged entities must apply when performing DD procedures. These measures have been developed with the aim to compensate for the higher risk of money laundering or terrorism financing.

Furthermore, in the third Directive the European Legislator implemented a section (the number 4) to regulate the CDD performed by third parties. This section was realized in order to define specific requirements that must be met by obliged entities and their third parts. Following Fernández Salas (2005) the permit to rely on third parts was issued "to avoid repeated customer identification procedures, leading to delays and inefficiency in international business"[187]. The Directive clearly illustrate that the responsibility for meeting the CDD requirements "shall remain with the institution or person covered by this Directive which relies on the third party"[188]. The third parties, in order to have the authorization to execute the

[184] Article no. 11, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.
[185] Article no. 13, comma 1, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.
[186] Article no. 13, comma 4, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.
[187] *The third anti-money laundering directive and the legal profession*, M. Fernández Salas, October 2005.
[188] Article no. 14, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.

due diligence, must be entities subjected to the directive's duty or, if from another country, to equivalent regulation.

5.4. Other Directive's requirements

The third Directive has developed the reporting procedures too. In chapter number III the Directive regulated the new reporting duties; first of all, the Legislator has introduced the mandatory establishment of a FIU, for each State Member, as a national center unit. The Directive has also clearly identified the specific functions that the Financial Intelligence Units have to comply with. These duties are the following: the FIU "shall be responsible for receiving (and to the extent permitted, requesting), analyzing and disseminating to the competent authorities, disclosures of information which concern potential money laundering, potential terrorist financing or are required by national legislation or regulation"[189]. The Directive established also that the FIUs have to have access to appropriate financial resources in order to perform the assigned activities. Furthermore, with the aim of providing to the FIUs all the necessary tools to combat money laundering and terrorism financing, Member States should provide the access "directly or indirectly, on a timely basis, to the financial, administrative and law enforcement information"[190] to the FIUs.

The FIUs are, at the Directive publication, growing in importance and are at the center of the suspicious transaction reporting scheme. Following Mitsilegas and Gilmore (2007) the "suspicious transaction reporting is now viewed within the

[189] Article no. 21, comma 2, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.
[190] Article no. 21, comma 3, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.

specific context of FIUs, as the institutions and persons involved must now send suspicions not to the competent authorities, but to the FIU[191]". The FIUs have also the possibility to exchange information with FIUs of other countries, which belong to the Edgemont Group network or to the European FIUs system. The Directive underlines that the international cooperation is considered a key point on the fight against ML and TF and established that "the Commission shall lend such assistance as may be needed to facilitate coordination, including the exchange of information between FIUs within the Community"[192].

The third Directive issued a series of complementary measures to the duties already covered (the Due Diligence and the suspicious transaction reporting). Following Fernandez Salas (2005) "these supporting measures essentially relates to record keeping, internal policies and procedures and to training"[193]. The record keeping chapter in the Directive is number IV. The European legislator required to the obliged entities, in Article no. 30, to keep the documents and/or information for at least five years, such as the copy or the references of the evidence collected or original documents or copies admissible in court proceedings. The regulator underlines the aim of this record keeping rules, which was established "for use in any investigation into, or analysis of, possible money laundering or terrorist financing by the FIU or by other competent authorities in accordance with national law"[194]. Thus, the Directive required that obliged entities must have "systems in place that enable them to respond fully and rapidly to enquiries from the FIU, or from other authorities"[195].

The Directive's chapter Enforcement Measures no. V, issued a series of provisions, divided into sections, on the *internal procedures, training and feedback, supervision, cooperation* and *penalties.* One of the most important

[191] T*he EU Legislative Framework against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards*, V. Mitsilegas and B. Gilmore, Cambridge University press, 2007.

[192] Article no. 38, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.

[193] *The third anti-money laundering directive and the legal profession*, M. Fernández Salas, October 2005.

[194] Article no. 30, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.

[195] Article no. 32, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.

obligations in this chapter was illustrated in Article no. 34, where the Legislator requested to the obliged entities to "establish adequate and appropriate policies and procedures of customer due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication in order to forestall and prevent operations related to money laundering or terrorist financing"[196]. The chapter focused also on the employees' importance on the Directive requirements. Anti-money laundering regulations have been developed many times through these years and it was really important that the obliged entities' employees were aware of the norms that have to be applied. Being the employees a fundamental element for combating ML and TF the third Directive established that the relevant employees have to participate at "special ongoing training programmes to help them recognize operations which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases"[197].

5.5. The Italian third Directive related regulation

As aforementioned the third Directive has been transposed in Italy in two Legislative Decrees: the first one related to combating terrorism financing, the Legislative Decree no. 109 of June 22nd, 2007; and subsequently the second one referred to the AML Directive's part, the Legislative Decree no. 231 of November 21st, 2007. Both Legislative Decrees have transposed and implemented the European Directive's obligations in Italy.

[196] Article no. 34, comma 1, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.

[197] Article no. 35, comma 1, Directive (EU) 2005/60/EC of the European Parliament and of the Council, October 26th, 2005.

The so called Anti-Terrorism Decree introduced in Italy the international standards developed to commonly fight terrorism financing. It introduced new duties for the already established *Comitato di Sicurezza Finanziaria,* which from June of 2007 have, as already covered in chapter no. 2.3, the aim of monitoring the TF and ML prevention systems and elaborates the strategies to counter it. Article no. 4 of the Decree, following the United Nation Security Council's resolutions, issued also the right to size money and other economic resources to people and companies suspected of terrorism financing.

The Italian anti-money laundering Decree, the no. 231 of November 21st, 2007, transposed the AML section of the EU Directive 2005/60/EC. It updated significatively the whole AML system, in order to implement the innovations brought by the third EU Directive. The Decree no. 231 established the Italian FIU, titled *Unità di Informazione Finanziaria* that replaced the *UIC* (which until the Decree publication was responsible for the Italian AML related measures and practices). The *UIF* institution was needed to comply with the AML European Standards, for this reason the *UIF* was in charge of the tasks defined in the third Directive. The Decree gave also to the supervision authorities the duty to promote and verify if the obligation issued in the text were respected by the obliged entities. They were in charge of sanctioning powers too. Furthermore, the Italian Decree implemented a stricter standard than the European one: the Italian AML Decree limited the use of cash and bearer bonds, in Article no. 49, defining the threshold for the cash payment to EUR 5 000 maximum.

CHAPTER VI: THE FOURTH EUROPEAN DIRECTIVE

The European anti-money laundering framework has been, since the first EU Directive, under constant development to remain relevant. Money launderers are constantly innovating their methods of laundering; terrorist financers have done the same. The technological progress is mutually advantageous to regulators and criminals. The FATF reviewed and updated its Recommendations, the latest update published in February 2012. Furthermore, according to Borlini (2015) the Legislator also addressed "the gaps highlighted by a 2011 report on the implementation of the third AML Directive"[198]. Thus, as already implemented in the previous Directives, based on the updated Recommendations, the European Legislator decided that there must be a revision of the Third Directive. On the May 20th, 2015 was issued the EU Directive 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial systems for the purposes of money laundering and/or of terrorist financing.

The Fourth Directive introduced the extension of the obligations to the whole gambling sector (the *"providers of gambling services"*), and further introduced the tax crime as predicated offences for money laundering crimes. As reported by Godinho Silva (2019) "the adoption of the 4th AML Directive was an important step in improving the EU's efforts to combat the laundering of money and to counter the financing of terrorist activities"[199].

The revised 2012 FATF Recommendations intention, following De Koker (2013), "was not to effect a radical change, but rather to clarify the existing

[198] *The Reform of the Fight Against Money Laundering and Terrorism Financing: From the 2012 FATF Recommendations to the New EU Legislation,* L. Borlini, Giuffrè Editore, 2015.

[199] *Recent developments in EU legislation on anti-money laundering and terrorist financing*, New Journal of European Criminal Law, Vol. 10(1) 57–67, P. Godinho Silva, 2019.

Recommendations, strengthen their consistency"[200]. The ML and TF Recommendations were integrated into this 2012 revised text. The Recommendations were developed following the risk-based approach. Recommendation no. 1 forced the Countries to *identify, assess, and understand* the ML and TF risks to which they are exposed, in order to "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"[201]. The aim adopted by FATF is to achieve an efficient allocation of resources, in order to implement an effective AML system.

6.1. The Directive's requirements

Compared to the Third Directive, the Fourth Directive introduced significant developments. The Directive has further implemented the risk-based approach, applying a more concise and articulated structure than the previous Directive. In order to adopt the adequate procedures, the Member States, as defined in the FATF Recommendations should "take appropriate steps to identify and assess the risks of money laundering and terrorist financing"[202]. Once the risks are assessed by the Countries, the Directive provides an additional step: the obliged entities must advance their internal procedures. This duty was covered in Article no. 8, comma 3 of the Directive. The European Legislator outlined that the obliged entities should "have in place policies, controls and procedures to mitigate and

[200] *The 2012 Revised FATF Recommendations: Assessing and Mitigating Mobile Money Integrity Risks within the New Standards Framework*, Washington Journal of Law, Technology & Arts, L. De Koker, 2013.

[201] FATF Recommendation "*International standards on combating money laundering and the financing of terrorism & proliferation"*, February 2012.

[202] Article no. 8, comma 1, Directive (EU) 2015/849 of the European Parliament and of the Council, May 20th, 2015.

manage effectively the risks of money laundering and terrorist financing identified at the level of the Union, the Member State and the obliged entity"[203]. Consequently, obliged entities must also assess the risks to which they are exposed, to develop the adequate policies, controls, and procedures accordingly. Logically, these policies must be defined proportionately to the *nature and size of the obliged entities.*

Regarding the CDD procedures the Fourth Directive innovated some particular elements. The Directive declared a date[204] for all anonymous accounts, anonymous passbooks, and anonymous safe-deposit box owners, by which they must be subjected to the CDD measures, to unauthorize the anonymity. In the third Directive the EU Legislator defined set circumstances, and customer categories, in which an obliged entity could perform the simplified CDD, without establishing the customer's risk level. The fourth Directive improved this step: it required the obliged entities to always assess the risk level of the customer before applying the simplified due diligence; as outlined in the text "before applying simplified customer due diligence measures, obliged entities shall ascertain that the business relationship or the trans action presents a lower degree of risk"[205]. Following E. and R. Camilleri (2017), obliged entities must "carry out a risk assessment notwithstanding the customer would, on the face of it, fall within the scope of the simplified customer due diligence client category"[206]. The Regulators objective was to ensure that the obliged entities were always assessing the risk level of a customer, preventing some customers being misrepresented in the simplified CDD procedure, however, they should be categorized as a medium/high risk. Furthermore, the Directive released, in Directives Annex II, the minimum factors that obliged entities must consider when establishing their customers risk level. These factors are divided into three categories, and each category establishes a series of sub-factors: "customer risk factors; product,

[203] Article no. 8, comma 3, Directive (EU) 2015/849 of the European Parliament and of the Council, May 20th, 2015.
[204] Also, in the previous Directive the EU Legislator asked to obliged entities to identify the owners of anonymous products, but without establishing a specific date.
[205] Article no. 15, comma 2, Directive (EU) 2015/849 of the European Parliament and of the Council, May 20th, 2015.
[206] *Accounting for Financial Instruments,* Emanuel Camilleri and Roxanne Camilleri, Routledge, 2017.

service, transaction, or delivery channel risk factors; and geographical risk factors"[207]. The enhanced CDD has been developed too: in the Third Directive the duty was regulated only in Article no. 14, while in the Fourth Directive it was regulated by Article no. 18 to Article no. 24. The fourth Directive published more detailed enhanced DD procedures, which obliged entities must comply with. Enhanced DD must not be performed automatically; if, after the risk assessment, the customer is considered as high-risk, the enhanced DD must be applied. The Directive established a series of obligations for specific circumstances that must be performed. Some of these circumstances are as follows: examination of background and purposes of all transactions; involvement of high-risk third countries; with respect to cross-border correspondent relationships, involvement of the execution of payments with a third-country respondent institution; involvement of politically exposed persons. Moreover, as for the simplified DD, the EU Legislator issued an Annex III with the factors, and types of evidence of potentially high-risk situations.

The fourth Directive listed for the first time, in Article no. 3, the functions/jobs that belong to the politically exposed persons category. In addition to the preceding Directive, in the fourth Directive, the EU Legislator considered PEP, the persons who are "no longer entrusted with a prominent public function by a Member State or a third country, or with a prominent public function by an international organization … for at least 12 months"[208]. The AML Directive further established that the "family members or persons known to be close associates of politically exposed persons"[209] must be considered as high-risk, and therefore as PEPs. Thus, for said persons it is required that the enhanced due diligence must be performed also for the next twelve months from the day in which they ceased to hold a position. As previously covered, before a PEP involvement an enhanced DD is always required, regardless their country of residence[210].

[207] Annex II, Directive (EU) 2015/849 of the European Parliament and of the Council, May 20th, 2015.
[208] Article no. 22, Directive (EU) 2015/849 of the European Parliament and of the Council, May 20th, 2015.
[209] Article no. 23, Directive (EU) 2015/849 of the European Parliament and of the Council, May 20th, 2015.
[210] In the third Directive the enhanced DD duties were performed only to PEPs residing in other Member States or in third countries.

The Directive highlights, in chapter no. III, the theme of Ultimate Beneficial Ownership. The Directive established that all corporate and legal entities (also trusts and other types of legal arrangements) incorporated within Member States "are required to obtain and hold adequate, accurate and current information on their beneficial ownership"[211]. All Member States, to comply with the Directive's obligations, must establish a central or public register with all the UBOs information. Member States must require that this register "can be accessed in a timely manner by competent authorities and FIUs"[212]. Additionally, the Directive established that for specific circumstances the register can be also be accessible for obliged entities, within the framework of customer due diligence, and for any member of the general public[213].

6.2. The Italian Fourth Directive related regulation

The European fourth Directive had to be transposed by the Member States until June 26th, 2017. Italian Government transposed the IV Directive into national law on May 25th, 2017 with the Legislative Decree no. 90. The Decree amended the previous two, on TF and ML (the 109/2007 and the 231/2007), implementing the several European innovations to the Italian framework.

Firstly, the Italian Decree established that the *Comitato di Sicurezza Finanziaria* was responsible in identifying, assessing, and evaluating the national money laundering and terrorist financing risks (Art no. 14). The Decree further introduced

[211] Article no. 30, comma 1, Directive (EU) 2015/849 of the European Parliament and of the Council, May 20th, 2015.

[212] Article no. 30, comma 2, Directive (EU) 2015/849 of the European Parliament and of the Council, May 20th, 2015.

[213] At least the following register information mentioned in Article no. 30, comma 5: the name, the month and year of birth and the country of residence and nationality of the beneficial owner as well as the nature and extent of the beneficial interest held.

that obliged entities must periodically assess the ML and TF risks that they are exposed to, so as to adopt procedures proportionately to the risk exposure level.

Concerning the obliged entities listed in Article no. 3, following the innovation of IV Directive, the Italian Decree introduced into national regulation the European financial intermediaries operating cross-border, and the providers of gambling services. With the aim to support the gambling service providers Article no. 54 ensures the involved institutions develop technical regulation standards, which must be respected. The Italian regulator transposing the Directive issued specific provisions to the providers of exchange services between virtual currencies and fiat currencies. In doing so, the EU and Italian Legislators attempt to regulate the virtual currency market, which in preceding years, due to vast technology development, has seen a considerable growth.

The customer due diligence topic is covered in Articles no. 17 to no. 29. The Legislative Decree details the CDD related procedures and obligations. The Decree no. 90 added several details throughout the entire CDD system. Some key updates are: the Legislator introduced the possibility to identify a non-face-to-face customer using a simple method if they have a digital identity, or a digital signature. The Decree revised the simplified DD section without defining the circumstances in which the simplified DD should be performed automatically, underlining that obliged entities must always assess the customers' risk level and choose which CDD to perform, only when the risk level is correctly assessed. The Italian Legislator issued some factors and criteria (such as the customer typology, products sold, services offered, and some geographical criteria), which obliged entities may choose to follow to help assess their customer's risk level. Obliged entities, in order to comply with the Decree no. 90, must internally define[214] the procedures and patterns to be implemented, with the aim to identify the circumstances in which, once the risk level is assessed, the simplified CDD should be performed. The Fourth Directive requested the Member States to implement a register with all the UBOs information; the Decree 90/2017 established the implementation of registering UBOs, however, the Italian

[214] Following their sector supervisory authorities' suggestions.

regulators have delayed the process because at the time of writing the register is yet to be implemented.

With the objective to remain current, the European Union began developing another Directive, meanwhile, in Italy the Fourth Directive was being implemented. The EU Legislator issued the fifth European AML Directive in 2018, the contents of which have been covered in the first part of the thesis.

CHAPER VII: FUTURE PERSPECTIVES

The European Union and the FATF have developed a stable framework of laws and regulations, aiming to reduce the money laundering phenomenon. However, crime, thus money launderers, never sleeps. Criminal organizations and international money launderers, as aforementioned, constantly attempt to develop new and innovative methods to launder their money, designing the most effective system.

On July 24th, 2019, the Commission approved a communication to the European Parliament and the Council, for better implementation of the EU's anti-money laundering and countering the financing of terrorism framework. This communication expressed the concerns of the European Commission regarding the "risks of money laundering and the financing of terrorism", as they definitely "remain a major concern for the integrity of Union's financial system and the security of its citizens"[215]. The EU Commission further highlighted that the money laundering and terrorism financing fight is "therefore an important priority for the Union and part of delivering the Security Union". The latest Directives were issued in quick succession, to increase the time of development for the regulatory framework. In 2018, the EU Parliament published a Sixth Directive[216]; the Directive issued a further list of predicate offences, and, following the EU Commission it "complements this preventive framework by harmonizing the definition of the criminal offence of money laundering and related sanctions"[217]. Following Koster (2020), the Sixth Directive, issued a total of twenty-two predicate

[215] *Communications from the Commission to the European Parliament and the Council towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework,* European Commission, July 24th, 2019.

[216] *Directive (Eu) 2018/1673 of the European Parliament and of the Council* of 23 October 2018 on combating money laundering by criminal law.

[217] *Communications from the Commission to the European Parliament and the Council towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework,* European Commission, July 24th, 2019.

offences, from December 2020 (the Directive had to be transposed by the Member States in December 2020), including: “environmental crimes, tax crimes and cybercrime, trafficking of drugs and humans and fraud”[218], broadening the scope of the AML laws.

The Commission emphasized areas needing improvement for the European Council, in order to improve the AML system. In the communication from the Commission, it highlighted the results from a EU report: the report on the assessment of recent alleged money laundering cases involving EU credit institutions[219]. The results exposed problems related to some cases analysis. Firstly, the report identified “incidents of failures by credit institutions to comply with core requirements of the Anti-Money Laundering Directive, such as risk assessment, customer due diligence, and reporting of suspicious transactions and activities to Financial Intelligence Units”[220]. It was assessed that the commitment of the obliged entities had discrepancies with the effort applied by each obliged entity. It was found some entities aimed to go beyond what was required, and fought against money laundering, whereas, others put limited effort and did not abide the rules. To ensure the development of an effective European AML system, it is vital that all the obliged entities of the Directives duties comply with the norms and regulations. Moreover, the Member States should commit themselves to comply with the Directives duties. However, it is not always the case: the EU report identified some cases in which the FIUs failed to apply the norms too. The FIUs evaluation was revealed in the report from the Commission to the European Parliament and the Council, assessing the framework for cooperation between Financial Intelligence Units[221]. The report exposed how some FIUs failed to “engage in a meaningful dialogue with obliged entities by giving quality feedback on suspicious transaction reports”[222]. This was not an

[218] *Towards better implementation of the European Union’s anti-money laundering and countering the financing of terrorism framework,* H. Koster, Journal of Money Laundering, Leiden University and Erasmus University Rotterdam, February 2020.

[219] The report *COM (2019) 373 final* of July 24th, 2019.

[220] *Communications from the Commission to the European Parliament and the Council towards better implementation of the EU’s anti-money laundering and countering the financing of terrorism framework,* European Commission, July 24th, 2019.

[221] The report *COM (2019) 371 final* of July 24th, 2019.

[222] *Communications from the Commission to the European Parliament and the Council towards better implementation of the EU’s anti-money laundering and countering the financing of terrorism framework,* European Commission, July 24th, 2019.

isolated FIU error, the EU Commission has also determined that several FIUs failed to cooperate with other countries' FIUs, without exchanging the requested information. Being the European (and International) cooperation one of the AML discipline pillar, it is imperative that each Financial Intelligence Unit cooperate with other FIUs. The Commission underlined that some technical problems and lack of regulations regarding the exchange of information, may be at the center of the failures. Member States' governments should implement and improve their Financial Intelligence Units operations, with the intention to encourage the exchange of information, which is intrinsic in the fight against money laundering.

To conclude, as covered in this thesis, the anti-money laundering and terrorism financing fight requires continuous revisions and updates. The European Legislator, in cooperation with the FATF and other international institutions, must closely monitor the theme and be ready to issue new Directives and regulations. The current framework against ML and TF has been efficaciously implemented, demonstrating the capability of the Legislators. Correspondingly, it is necessary that the laws and regulations are correctly realized, it is not sufficient to just issue new laws. Therefore, the European institutions have to monitor the application of the regulations, and take action where necessary, consequently eliminating the identified vulnerabilities. With an outlook to the future, the role of the Legislator will become increasingly difficult, as a balance between costs and benefits must always be reached. Obliged entities have to be efficient, their compliance employees' teams and organizational units can be costly and sometimes, to ensure total compliance with the norms, can require significant effort. The ability of the regulator is to balance the achievements, whilst simultaneously maximizing effectiveness.

Reference list

A. Becchi and G. M. Rey (1994), L'economia criminale, Laterza.

A. Verhage (2011), The anti-money laundering complex and the compliance industry, Routledge.

B. Unger (2007), Money Laundering, Tax Evasion, Capital Flight, Tax Havens, the Rule based and the Risk Based Approach: Keep it Simple, Utrecht School of Economics.

B. Unger and F. Van Waarden (2009), Review of Law & Economics: How to Dodge Drowning Data? Rule- and Risk- Based Anti-Money Laundering Policies Compared, Utrecht University School of Economics, Bepress.

C. Ciampi, F. Berghella, G Conforti, U. Fava, E. Granata, C. Lauria, A. Lo Monaco, A. Pansa (1998), Nuova guida agli adempimenti antiriciclaggio e antiusura, manuale operativo per le banche, gli intermediari finanziari, i sindaci e gli amministratori, Bancaria editrice.

C. Jojarth (2013), Transnational Organized Crime, analyses of a global challenge to democracy, Transcript Verlag.

Communications from the Commission to the European Parliament and the Council towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework, European Commission, July 24th, 2019.

Council Framework Decision on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime, 2001/500/JHA, of June 26th, 2001.

Customer due diligence for banks, Basel Committee on Banking Supervision, Working Group on Cross-border Banking, Bank for International settlements, October 2001.

D. Cox (2014), Handbook of Anti Money Laundering, Wiley.

D. E. Teitelbaum and K. F. Kaufmann (2003), Current developments in anti-money laundering laws, American Bar Association.

D. Hopton (2009), Money laundering: A concise guide for all business, Taylor & Francis Group.

D. Masciandaro (1995) Economia del riciclaggio e della politica antiriciclaggio, Giornale degli economisti e annali di economia, EGEA SpA.

Directive (EU) 2001/97/EC of the European Parliament and of the Council of December 4th, 2001.

Directive (EU) 2005/60 of the European Parliament and of the Council of October 26th, 2005.

Directive (EU) 2015/849 of the European Parliament and of the Council of May 20th, 2015.

Directive (EU) 2018/1673 of the European Parliament and of the Council of October 23rd, 2018 on combating money laundering by criminal law.

Directive (EU) 2018/843 of the European Parliament and of the Council of May 30th, 2018.

Directive (EU) 91/308/EEC of the Council of June 10th, 1991.

Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo, Bank of Italy, 30 Luglio 2019.

Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo, Banca d'Italia, 26 Marzo 2019.

E. U. Savona (1997), Responding to Money Laundering International Perspectives, Harwood academic publishers.

E. V. Mulig and L. M. Smith (2008), Understanding and Preventing Money Laundering, working paper.

European Banking Authority, Consultation Paper of February 5th, 2020.

FABI (Federazione autonoma bancari Italiani) (1993), Le leggi antiriciclaggio.

FATF (2008), Risk-based approach guidance for Legal Professions, Paris.

FATF (2013), Guidance, Politically Exposed Persons, Paris.

FATF (2014), Guidance, Transparency and Beneficial Ownership, Paris.

FATF (2014), Risk-based approach guidance for the banking sector, Paris.

Financial Action Task Force (Updated October 2020), The FATF Recommendation report: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, 2012.

First Commission's report on the implementation of the Money Laundering Directive (91/308/EEC) to be submitted to the European Parliament and to the Council, Commission of the European Communities, COM (95) 54 final, 1995.

G. M. Rey (2018), Interazioni fra economia criminale e economia legale.

General Assembly 55/25 United Nations Convention Against Transnational Organized Crime, 8th January 2001.

H. Koster (2020), Towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework, Journal of Money Laundering, Leiden University and Erasmus University Rotterdam.

I nuovi obblighi antiriciclaggio, guida per professionisti ed intermediari, Il Sole 24 Ore focus norme & tributi, 20 Marzo 2019.

International Convention for the Suppression of the Financing of Terrorism

Adopted by the General Assembly of the United Nations in resolution 54/109 of December 9th, 1999.

J. Ferwerda (2008), The Economics of Crime and Money Laundering: Does Anti-Money Laundering Policy Reduce Crime?, Tjalling C. Koopmans Research Institute, Utrecht School of Economics.

J. Vyhnálik and I. Fendeková (2005), Legislation of the European Union, The Third Eu Directive on Money Laundering and Terrorist Financing, Volume XIII, National Bank of Slovakia.

L. Borlini (2012), EU Anti-money Laundering Regime: An Assessment within International and National Scenarios, Research Paper Series No. 2012-125.

L. Borlini (2015), The Reform of the Fight Against Money Laundering and Terrorism Financing: From the 2012 FATF Recommendations to the New Eu Legislation, Giuffrè Editore.

L. De Koker (2013), The 2012 Revised FATF Recommendations: Assessing and Mitigating Mobile Money Integrity Risks within the New Standards Framework, Washington Journal of Law, Technology & Arts.

L. Di Brina and M. L. Picchio Forlati (2002), Normativa Antiriciclaggio e contrasto della criminalità economica, CEDAM.

La Disciplina dell'Antiriciclaggio e gli Adempimenti dei Professionisti, a cura del Consiglio Nazionale Dottori Commercialisti, il Sole 24 Ore.

Law no. 197, July 5th, 1991.

Legislative Decree no. 109 of June 22nd, 2007.

Legislative Decree no. 125 of October 4th, 2019.

Legislative Decree no. 143 of May 3rd, 1991.

Legislative Decree no. 231 of November 21st, 2007.

Legislative Decree no. 56 of February 20th, 2004.

Legislative Decree no. 90 of May 25th, 2017.

M. Barbieri (2019), Europeizzazione e convergenza di policy design: evoluzione e consolidamento delle politiche antiriciclaggio in Italia, Il Mulino.

M. Fernández Salas (October 2005), The third anti-money laundering directive and the legal profession.

M. Frankl and A. E. Kurce (2016), Money Laundering and Terrorist Financing Activities, Business Expert Press.

M. Levi and P. Reuter (2006), Crime and Justice, Vol. 34, The University of Chicago Press.

M. Pacini (2000), Il controllo pubblico antiriciclaggio in Italia: recenti riforme e prospettive, Il Mulino.

M. Young (2013), Banking Secrecy and Offshore Financial Centers, Money laundering and offshore banking, Routledge.

MEF Decree no 141 of February 3rd, 2006.

N. M. Healy (2002), The International Lawyer, the impact of September 11 on Anti-Money Laundering Efforts, and the European Union and Commonwealth Gatekeeper Initiatives.

P. Costanzo (2007), Rule-Based vs. Risk-Based approaches to control. The third EU AML/CFT Directive Conference, Utrecht School of Economics.

P. Godinho Silva (2019), Recent developments in EU legislation on anti-money laundering and terrorist financing, New Journal of European Criminal Law, Vol. 10(1) 57–67.

P. Meagher (October 2019), Risk-based Customer Due Diligence, technical notes CGAP.

P. Reuter and E. Truman (2004), Chasing Dirty Money: The Fight Against Money Laundering, Peterson Institute for International Economics.

Quaderni di Ricerca Giuridica, Lineamenti della disciplina internazionale di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, Banca d'Italia, Febbraio 2008.

R. Razzante (1999), La normativa Antiriciclaggio in Italia, Giappichelli Editore.

Rapporto Annuale 2019, Unità di Informazione Finanziaria per l'Italia, Roma, Maggio 2020.

Regolamento (CE) n. 1889/2005, regolamento del Parlamento Europeo e Consiglio relativo ai controlli sul denaro contante in entrata nella Comunità o in uscita dalla stessa; 26 ottobre 2005.

Relazione al Ministro dell'economia e delle finanze del Comitato di sicurezza finanziaria, valutazione delle attività di prevenzione del riciclaggio e del finanziamento del terrorismo, Ministero dell'Economia e delle Finanze, anno 2007.

Report from the Commission to the European Parliament and the Council assessing the framework for cooperation between Financial Intelligence Units, report COM (2019) 371 final of July 24th, 2019, Brussels.

Report on the assessment of recent alleged money laundering cases involving EU credit institutions, report COM (2019) 373 final of July 24, 2019, Brussels.

S. Betti (2001), The European Union and the United Nations Convention against Transnational Organized Crime, working paper, European Parliament.

S. Iacolino (2013), Documento di lavoro sul riciclaggio di denaro, Commissione speciale sulla criminalità organizzata, la corruzione e il riciclaggio di denaro, Parlamento Europeo.

The Forty Recommendations, Financial Action Task Force on Money Laundering, 1996.

The Forty Recommendations, Financial Action Task Force on Money Laundering, 1990.

The Forty Recommendations, Financial Action Task Force on Money Laundering, 2003.

The identification of beneficial owner of legal entities in the fight against money laundering, Final Report of Project BOWNET, 2013.

The International Bank for Reconstruction and Development/The World Bank/ The International Monetary Fund (2006), Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism.

United Nations Office on Drugs and Crime (October 2011), Research Report “Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes”.

V. Mitsilegas and B. Gilmore (2007), The EU Legislative Framework against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards, Cambridge University press.

W. C. Gilmore (2011), Dirty Money, the evolution of international measures to counter money laundering and the financing of terrorism, Council of Europe Publishing.

Websites

Banca d’Italia, https://www.bancaditalia.it

Egmont Group website, https://egmontgroup.org/en

Financial Action Task Force, https://www.fatf-gafi.org

Unità di Informazione Finanziaria, https://uif.bancaditalia.it

United Nation Office on Drugs and Crime, https://www.unodc.org