UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M.FANNO"

CORSO DI LAUREA MAGISTRALE IN

Business Administration

TESI DI LAUREA

Money laundering and criminal connected firms: impact on bank lending activity

RELATORE:

CH.MO PROF. Antonio Parbonetti

LAUREANDO: Jacopo Roviaro

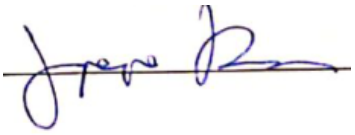
MATRICOLA N. 1106346

ANNO ACCADEMICO 2019 – 2020

Il candidato dichiara che il presente lavoro è originale e non è già stato sottoposto, in tutto o in parte, per il conseguimento di un titolo accademico in altre Università italiane o straniere.
Il candidato dichiara altresì che tutti i materiali utilizzati durante la preparazione dell'elaborato sono stati indicati nel testo e nella sezione "Riferimenti bibliografici" e che le eventuali citazioni testuali sono individuabili attraverso l'esplicito richiamo alla pubblicazione originale.

The candidate declares that the present work is original and has not already been submitted, totally or in part, for the purposes of attaining an academic degree in other Italian or foreign universities. The candidate also declares that all the materials used during the preparation of the thesis have been explicitly indicated in the text and in the section "Bibliographical references" and that any textual citations can be identified through an explicit reference to the original publication.

Firma dello studente



INDEX

Introduction

Money laundering still represents one of the main challenges that governments, central banks and legislators are asked to fight on a daily basis, despite the international efforts put in place to curb its spreading and rise. Indeed, the money laundering phenomenon extends on a huge scale: back in 2009, the United Nations Office on Crime hypothesized it to be ranged between 800 and 2 trillion dollars at global level, corresponding to a share between 2 and 5% of global GDP[1]. As outlined by the former Minister for the Economic Affairs Pier Carlo Padoan, in Italy money laundering is worth approximately between 30 and 240 billion Euros.

The recent cases documented in Italy, involving especially banks, increased the awareness towards the phenomenon and encouraged further investigations. Among the recent scandals, the case of ING Direct Italia is particularly significant. In 2019, ING Direct paid a fine of 30 million Euro to the Bank of Italy, with the objective to restore its business operations concerning the acquisition of new customers, as a consequence of the irregularities uncovered on behalf of the enforcement of anti-money laundering legislation.

Another interesting case arose from Cordusio Sim (Unicredit Group) in 2019, which was object of detailed investigations by the Bank of Italy, primarily due to its failure in respecting and in committing to the anti-money laundering procedures, and more specifically, in the lack of identification of the source of money from some of its richest customers, whose accounts held amounts exceeding the critical threshold.

However, banks are not the unique institutions involved in the phenomenon of money laundering, indeed, the latest scandals involved also a number of non-financial companies. For instance, the investigation held by the disruptive news organization Fanpage "Bloody Money", in 2018, unveiled and highlighted the illicit traffic of toxic waste and the laundering of the related proceeds in Northern Italy, including in this major scandal the Venetian area where we live, more precisely involving the cities of Venice and Verona[2].

Considering the above facts as a background of this study, the primary objective of this research is to investigate on the relationship between money laundering, the banking system and the companies that populate the Italian economic framework, with the final purpose to investigate and to measure the impact that money laundering cases might have on banking activities. To achieve this result, we will develop a statistical research on the data collected from the Italian municipalities, as part of a police operation that took place from 2005 to 2014, revealing a

[1] https://www.unodc.org/unodc/en/money-laundering/globalization.html
[2] http://www.veronasera.it/cronaca/fanpage-bloody-money-verona-13-marzo-2018.html

phenomenon of money-laundering related offenses, which were perpetrated by companies related to criminal organizations.

Our research will observe the effect of the criminal presence on bank lending activity, focusing especially on the Italian level of the phenomenon, in order to highlight if the former might somehow influence the latter, and in positive case, in which measure.

In Chapter 1, we will perform a literature review that investigate the topic of money laundering. Indeed, in order to build our research on a solid theoretical basis, we give a detailed definition of the phenomenon according to the most recognized sources of information, explaining how the process of money laundering is normally implemented by criminals. In order to build an even more detailed background for the research, we also investigate on the types of companies that have been historically more involved in money laundering, in order to understand their role and weaknesses.

In Chapter 2 we present the pillars of our on-field research, through an overview of the major literature written on the topic of money laundering within the current European legislation, in order to comprehend the role of financial and non-financial institutions in the fight against the phenomenon.

Ultimately, in Chapter 3 we develop our statistical analysis, for an in-depth investigation on the relationship between the criminal companies and the bank lending activity, with a geographical focus on the municipality level. The economic research at Italian level, and its related academic literature, provides clear evidence of the existing relationship between crime and bank lending activity. The ultimate purpose of our research is to verify if the data collected within our analysis are coherent and provide consistency to the existing economic literature on this topic.

First Chapter

Money laundering: definition and techniques

1.1 Introduction

To introduce the topic, an excursus is made throughout the primary definition of the Money Laundering phenomenon and its implementation in practical terms, highlighting the major steps that can be observed crosswise in every laundering process, with a certain recurrence and methodology.

Later in the chapter, we further investigate the different money laundering techniques explored by the literature, moving from the classic physical movement of cash, to the involvement of bank and non-bank financial institutions. Indeed, due to the increasing presence of anti-money laundering regulations implemented by the banking sector, launderers are moving their focus and increasing their attention towards non-bank financial institutions. The latter, being a less regulated sector, offers numerous opportunities to criminals for exploiting and accessing their illegal proceeds, leveraging on exchange services, remittance services, HOSSPs and insurance services. Other vulnerable sectors, lacking of regulatory systems and preventive measures, involve the non-financial businesses as well as the electronic transfers of funds and cryptocurrencies.

As a conclusion, the phenomenon of money laundering among companies is analysed as, in some industries more than others, suspicious or fraudulent movements of money might be registered between different entities. Therefore, we investigate on the main methodologies and strategies adopted by launderers to disguise their illegal operations and to divert the financial system regulation, with the objective to create an inflow of illicit liquidity inside the industry, or across different industries.

1.2 Money laundering definition

Money laundering is a phenomenon that finds numerous definitions and formulations in literature. One of the major theoretical contributions tends to define it as "*the process by which one conceals the existence, illegal source, or illegal application of income, and then disguises*

that income to make it appear legitimate"[3]. Moreover, the definition of the Interpol cites "*any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources*"[4]. However, the majority of countries tends to adopt a more detailed definition, which was formulated by both the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (*Vienna Convention*) and the United Nations Convention Against Transnational Organized Crime (2000) (*Palermo Convention*):

- *"The conversion or transfer of property, or from an act of participation in such offence or offences, 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 offence or offences to evade the legal consequences of his actions;*
- *The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offence or from an act of participation in such an offence or offences, and;*
- *The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime"*[5]*;*

We can highlight a common feature between the above definitions: the ultimate purpose of the Money Laundering phenomenon is the concealment or camouflaging of income generated from any type of illegal activities. Indeed, in general terms, criminals have the major interest to erase any proof of their misbehavior and, simultaneously, need a direct access to the money collected unlawfully, in order to profit from illicit activities. Money laundering is a deceitful activity, applied with the principal purpose to misdirect the administrative authorities from the legal genesis of illicit income, as well as from its consequent owner.

The Vienna Convention's definition of Money Laundering might be defined as too restricted, as it specifically focuses on those underlying activities from which the criminal proceeds arise, e.g. the traffic of drugs, without contemplating any unrelated crime, e.g. fraud, kidnapping or robbery.

Therefore, the Palermo Convention aimed at extending the previous definition by detailing a long list of predicate offenses, while highlighting that profits arising from the traffic of drugs are just an example among many types of laundered funds.

[3] President's Commission on Organized Crime – Interim Report to the President and the Attorney General (1984), "*The cash connection: Organized Crime, Financial Institutions, and Money Laundering"*

[4] https://www.interpol.int/Crime-areas/Financial-crime/Money-laundering

[5]http://siteresources.worldbank.org/EXTAML/Resources/396511114658142787 1/Reference_Guide_AMLCFT_2ndSupplement.pdf

Notwithstanding the crime, the literature[6] highlights a three-stages approach adopted by the launderers for turning their illicit proceeds into apparently clean money or assets:

- *Placement* is the first step, involving the physical and actual movement of illegally sourced funds, towards a place or within a form that results less suspicious at the eyes of the law enforcement authorities. This is principally achieved either through the introduction into the financial system, or through traditional or non-traditional financial institutions, or alternatively, leveraging on the retail economy. In practice, this is obtained by depositing cash into a bank account: firstly, any large amount of cash is split into many small amounts, secondly, their deposit is staggered over time and among many different offices of financial institutions. Moreover, there is a possibility that illegal funds are converted into financial instruments, such as checks, and paired to other legitimate funds in order to discourage suspicion; furthermore, they could be used to purchase a security or an equivalent form of insurance contract. The act of placement has two specific purposes: to avoid its detection by authorities and to move money as far as possible from its illicit source.
- *Layering* is the second step that encourages the separation of gains from their illegal roots, throughout a multitude of financial transactions that blurs the audit trail of the proceeds. Once illegally-obtained money is introduced to the financial system, it is repeatedly converted or transferred towards other institutions, with the objective to place it further and further from its criminal source. Those funds may either be implied to purchase other financial instruments or any other type of investment instrument, as long as it is easily transferable. Alternatively, the illicit funds can be either transferred through negotiable instruments, i.e. checks, money orders or bearer bonds, or also transferred electronically to new bank accounts under other jurisdictions. To conclude, the act of layering implies the creation of a web of financial transactions, that reflects the one of a legitimate financial activity, both in terms of frequency, complexity and amount.
- *Integration* is the third and final step, involving the inclusion of illicitly sourced funds into the legitimate economy. It is achieved by purchasing a variety of assets, such as real estates, financial assets, and other types of goods, with the final aim to convert these funds into apparently licit business earnings, that may arise from a normal financial or commercial operations system.

[6] Schott, P. A. (2006), "*Reference Guide to Anti-money laundering and Combating the Financing of Terrorism (Second Edition)*", Business and Economics.

After the examination of the three-stages approach, it results clear that money laundering is not just the process of blurring the proceeds arising from illegal activities: for launderers it is equally important to make the funds re-usable for other purposes. The laundering mechanism results to be especially vulnerable during the *placement* stage, mostly because those illegal activities generate a huge amount of money, which is difficultly disguised in numerous large amounts. Therefore, the launderer has to implement a technique to relocate large amounts of cash and turn them into more disposable forms, to be able to introduce them into the financial system. The principally-adopted technique is to use front corporations to deposit liquidity - as well as check cashing business solutions - with the aim to turn liquids into marketable instruments (i.e. travelers' checks, cashiers checks, money orders). Similarly, the function of offshore financial centers seems to play a central role in hiding the real source of illicit funds: in this case, funds are moved to offshore accounts, entering this way the banking system, and embracing various jurisdictions.

1.3 Money laundering techniques

Over the decades, money launderers implemented a multitude of techniques, that increased their level of sophistication at the same rate of the sharper and sharper regulation system that authorities put in place to contrast their illicit conduct.

The principal sources of illegal proceeds result to be, as always, drug trafficking and tax evasion[7]. However, non-drug related earnings are currently increasing in relevance, as a possible result of the higher compliance level obtained by banks with the implementation of anti-money laundering measures[8].

In this paragraph, the literature review goes through the most common money laundering techniques, by analyzing the three main industries involved in the process: banks, financial institutions other than banks, non-financial businesses.

1.3.1 Physical transportation of cash

The physical transportation of cash is the primary technique utilized by launderers, despite the fact of being the eldest, the most simple and, somehow, elementary way to practice money laundering.

There are both cultural end economic reasons for which cash is still the preferable method to

[7] FATF (2015), "*Money Laundering Through the Physical Transportation of Cash"*, Financial Action Task Force Report, page 30

[8] *FATF Annual Report 1996-1997*, page 7

purchase goods and services: primarily, this is an anonymous way to buy assets, and at the same time, in many countries it is a widely accepted payment method for low value trades.
Secondly, the economic benefits of cash transactions are numerous: they are quicker, they permit a certain degree of negotiation between the buyer and seller, and they reduce indebtedness and costs in terms of interest and fees[9].

1.3.2 The banking sector

The banking sector is the principal vehicle used by launderers to turn criminal proceeds into disposable amounts. The classic technique used for placement (for a definition, see Paragraph 1.2), in which large sums of cash were simply deposited into bank accounts, has been increasingly discouraged thanks to the likelihood of being signaled to the law enforcement authorities, that apply their supervision.
Indeed, placement was implemented through "smurfing", i.e. the act of splitting a huge transaction into many small transactions of limited amount[10], that being below the critical threshold, did not require any report to the attention of authorities. But, consequently, authorities decided to implement a currency transaction report which is required for any financial institution handling a transaction exceeding a certain amount of cash, even if it is below the critical threshold already settled.
Therefore, a new solution used by launderers was to create accounts under the name of their associates, relatives, or other persons who worked in their behalf, as well as shell companies located or established in other jurisdictions, with the objective to discourage and hamper the investigation of authorities.
Nowadays, shell companies are a particularly convenient instrument for money laundering, as they dissociate the illicit funds from the identity of their beneficial owner; moreover, they are normally set offshore or handled by professionals who hold information secrecy, eluding controls. Shell companies are implied both in the placement stage, when they receive large deposits of cash which are moved offshore, and during the integration stage for the purchase of real estates.
Moreover, the establishment of a "collection account" is an additional technique which is widely used especially by immigrants from Asia and Africa: many small amounts of money are payed to a bank account, then money is sent abroad to their homeland.

[9] *Money Laundering Through the Physical Transportation of Cash*, 2015, FATF Report
[10]Helmy, T., Abd-ElMegied, M. Sobh, T., Badran, K. (2014), *Design of a Monitor for Detecting Money Laundering and Terrorist Financing,* International Journal of Computer Networks and Applications, Volume 1, Issue 1, November – December, page 2

In many cases, this method of payment is used for legal and legitimate purposes by laborers and immigrants that work and send money back to their mother country. However, in some cases, the same channel is exploited by criminal groups to launder illicit funds by leveraging on this commonly spread phenomenon.

Moreover, the organized criminality tends to break into smaller banks, normally through an accomplice bank director or bank employee, by infiltrating into the business and recycling any bank account used for structuring purposes. Consequently, this bank account is used for frequent cash withdrawals, significant deposits and movements of cash, and after some months it is abandoned and extinguished. Only few thousand dollars are left into the account, throughout the period that comes before the audit of the account: therefore, during the audit, the bank will evidence small activities in the latest months, considering the account less suspicious.

In addition to it, international money launderers tend to use the method of "payable through accounts"[11], i.e. demand deposit accounts which are present at financial institutions on behalf of foreign banks or corporations. They act as a funnel of cheques, deposits and sums of money of all their customers that merge into a single account, which is held at the local bank by a foreign bank. Payable through accounts represent a significant threat of money laundering, especially for those local banks who are unable to set standard internal policies or internal reporting guidelines, in order to verify the trustworthiness of their customers.

To conclude, the last technique used at banks is the "loan back arrangement"[12]: here money launderers move their illicit funds offshore, and consequently they utilize them as a security or as a guarantee for bank loans, going back to their original country.

The proficiency and effectiveness of the loan back arrangement is high, as it allows launderers to dispose of funds - making them appear clean - benefiting from tax advantages too.

Besides the above-mentioned techniques, other important tools utilized at all stages of the laundering process are: telegraphic transfers, bank drafts, money orders and cashier's cheque. The high speed that characterizes these techniques is the major benefit registered by launderers, as it makes difficult for authorities to trace the illegal proceeds in a very rapid and immediate way.

1.3.3 Non-bank financial institutions

As evidenced in the previous paragraph, banks offer a wide range of tools on which criminals

[11] Stamp, J., Walker, J. (2007), "*Money laundering in and through Australia, 2004"*, Trends & Issues in crime and criminal justice No. 342, Australian Institute of Criminology, page 1

[12] Madinger, J. (2011), "*Money Laundering: A Guide for Criminal Investigators, Third Edition", page 257*

can leverage to launder money. As an alternative, non-bank financial institutions result to be equally attractive for introducing illegal proceeds into the financial system, especially because of the increasing effectiveness of the anti-money laundering regulatory actions put in place by banks.

1.3.3.1 Exchange services

Firstly, bureau de change and exchange offices represent a significant threat of money laundering, as they offer a wide range of services which are less regulated than the traditional financial institutions, and simultaneously, they are characterized by a general inadequate education and insufficient internal control systems. Therefore, exchange services are used to sell and buy foreign currency, exchange financial instruments, or to periodically consolidate many small bank notes into more consistent denomination bank notes. The occasional feature of these acts makes it even more complicated for operators to highlight any deceptive or suspicious activity, through the so called "know your customer" policy plans[13].

1.3.3.2 Remittance Services

Secondly, remittance services are another significant tool for money laundering, as they are normally subject to a lighter regulatory system with respect to banks but, at the same time, they offer equivalent services, even by charging a lower commission rate. The non-banking segment of the population, composed by expatriate workers and clandestine people, normally uses these services to transfer money to the developing countries, where the existence of banking services is almost null. Customers submit cash to the remittance service, that transfers it - through the banking system - to another account which is owned by an associate company in the country of destination, that turns it into available cash for the ultimate beneficiary.

1.3.3.3 HOSSPs and underground banking providers

Thirdly, several launderers also benefit from the system of *hawala*, *hundi* or from the *underground banking*[14], that differentiate themselves from the money remittance services thanks to the usage of non-bank services as a channel to transfer money, and are established within a long period of time.

"Hawala" is the naming of a money transfer methodology that originates in South Asia many

[13] McDonell, R. (1998), "*Money laundering methodologies and international and regional counter-measures"*, National Crime Authority, NSW, paper presented at the Australian Institute of Research, page 4

[14] McDonell, R. (1998), "*Money laundering methodologies and international and regional counter-measures"*, National Crime Authority, NSW, paper presented at the Australian Institute of Research, page 5

centuries ago, traditionally established as a closed system between families and tribes, where they settle a specific path or corridor for the flow of money.

Hawala and Other Similar Providers (also named HOSSPs) are legally recognized in some countries, while in others they are not licensed and considered as illegal. The services they provide are both legitimate and illegitimate, having many characteristics in common with other money transmitters[15]: they all are businesses with inflows and outflows of cash, operating with immigrant workers or clandestine people of a particular ethnic group, that form part of a network of operators among different countries. Their popularity is due to both speed and convenience of the money transfers: it takes from few hours to a couple of days to transfer money worldwide, and the service charge is cheaper than baking services, with costs amounting at 25-50% of the equivalent bank charge. There is also a cultural driver pushing people from Middle East and Central-South Asia to use the money transferring services: while living in developed countries, expatriate workers or immigrants can build relationships and long-term networks with the *hawala* service providers, who share with them a similar ethnic group and language.

The hawala system might be illegally exploited to transfer profits derived from criminal activities, to evade taxes as well as bank controls on cash deposits. Indeed, international transactions through banks are subject to certain restrictions, that are eluded in this way. Furthermore, there is no possibility for authorities to control the inflows and outflows of money through *hawala*, avoiding also the subjection to tax controls as there is no evidence of money in their bank account records.

The major issue for HOSSPs is the complete absence of any regulatory system, nor any compliance study or customer due diligence, that makes the transferring system very vulnerable towards money laundering.

Criminal HOSSPs methodology enrolls four actors in the process: a money-broker or controller, a collector of money, a coordinator and a transmitter. The character of the money-broker is usually active in several criminal organizations and different countries, and the responsibility embraces the full process, from the cash collection to the delivery. The second actor, the collector, strictly follows instructions taught by the controller: he meets the criminal actors and keeps the cash, being exposed to a high risk of being arrested. Once the cash is collected, the controller makes sure that an equivalent amount of money is available in the country of destination and arranges the transaction either with an electronic payment or with a physical

[15] *The role of Hawala and other similar service providers in money laundering and terrorist financing*, FATF Report 2013, page 11, http://www.fatf-gafi.org/publications/methodsandtrends/documents/role-hawalas-in-ml-tf.html

handover of cash. The third actor, the coordinator, is an intermediary person who manages a part of the laundering process. The money transmitting service is the fourth actor, who receives and transfers money to the controller.

The criminal activities from which proceeds arise are, generally, drug trafficking activities, that benefit from the speedy movement from one country to another, where drug cartels are established. For example, in the 1990s, the Colombian and Mexican drug cartels established a technique named "black market peso exchange"[16], with the aim to transfer and conceal the drug traffic profits gained from the US market. In this process, once drugs were sold in the United States, the Colombian or Mexican drug cartel put itself in contact with a peso broker, i.e. the controller of the operation, who bought the drug trafficking proceeds in US Dollars, from an agent based in the States, and then deposited an equivalent amount of money, this time in Pesos, inside the bank account of the drug cartels based in Colombia or Mexico.

1.3.4 Non-financial businesses

Given the constant revision and upgrade of the anti-money laundering regulation with respect to the financial sector, criminals are looking with unceasing attention to non-financial business in order to launder illicit funds[17]. Particularly, two business categories can be considered as suspicious activities for money laundering and for this reason more reporting measures must be taken to detect this kind of actions. We are talking about the gaming sector which includes all the activities related to gambling houses and bookmakers and the sellers of high value products as for instance artistic items and real estate. In the former case, businesses based on gambling activities give launderers the opportunity to carry out investment operations through a no-legitimate source apparently, making the threat for money laundering even more evident. Specifically, the process consists of buying chips with cash and getting the payment back with cheque drawn on the casino account; moreover, when more casinos located in different countries are involved, operations of buying and paying back can be carried out in different casinos making operations difficult to relate each other and trace.

1.3.4.1 Electronic fund transfers

The increasing use of online methods of payments and electronic fund transfers worldwide encouraged illicit and no-transparent operations that have been eased thanks to a lack of a

[16] Reuter, P. Truman, E. M. (2004), *Chasing dirty money, the fight against money laundering, Institute for International Economics*, page 36

[17] FATF (1995), *Annual Report 1994-1995*, pp. 17-18

harmonious suitability between national payment systems and SWIFT international system[18]. In this regard, getting personal information about the subjects involved in these operations represented a challenging task for government and law enforcement institutions for many years, since the financial system complexity and the huge amount of transactions within it make the activity of tracing unlawful movement of funds even more tricky.

As well as fund transfers performed by banks at international level, there are other cases in which money is transferred by remitters to less developed countries and with a low-quality and structure of the banking system[19]. Indeed, these transfers may be addressed to immigrants, clandestine foreigners and groups of people dealing with suspicious networks or illicit activities. In this way, money transfers to foster unlawful operations and money laundering are increasing and getting more and intense. Nevertheless, transfers of money not only concern networks or categories of people but also may be implemented through postal services network in which large sums are transferred in an anonymous way.

There are several ways allowing illicit transfers of electronic funds. It's the case for instance when different banks are involved in the operation and transfers are made with the aim to hide their origin and trail as well as when transfers are addressed to a principal collecting account located abroad and initial deposits have been made by avoiding their identification ("smurfing")[20].

1.3.4.2 Lawyers, notaries and accountants

Money laundering techniques represent a real issue in the legal and accounting sectors involving lawyers, notaries, advisors and financial intermediaries even more. In these sectors, indeed, many suspicious and deceitful operations may occur giving the opportunity to other legal entities and businesses to get into the process. There are several techniques used to carry on money laundering operations and elude the legislation system. One of these is to deposit amounts of money into the lawyer's clients account and use them to invest in real estate. Funds that have been deposited in the lawyer's client account may also be kept hidden in the form of cheque drawn through an offshore bank located abroad. Another technique is to transfer money in a country abroad where anti-money laundering regulations are very flexible or even no effective and later open several bank accounts under false identities and companies[21]. In this context, it has to be said that lawyers, notaries or other legal subjects, although having a role of

[18] FATF (1995), *Annual Report 1994-1995*, page 18
[19] FATF (1998), *Annual Report 1997-1998*, page 48
[20] FATF (1998), "*Annual Report 1997-1998"*, page 50
[21] FATF (1998), "*Annual Report 1997-1998"*, page 53

assurance and transparency in many legislations, may be indirectly involved in the process or may facilitate illegal procedures and transactions being completely unaware of the facts.

1.3.4.3 Gold and diamond market

Differently from money, the current global scenario is characterized by the use of raw materials and precious metals to carry on money laundering operations. One of the most used raw material is gold. At the base of its recourse there are some important characteristics[22]: high intrinsic value, the possibility to trade on world markets, its price is daily set, it can be converted, maintains its value despite its form (e.g. bullion or jewellery pieces) and transfers are potentially anonymous. Gold operations are mostly related to illegal groups and activities where gold is purchased with funds deriving from unlawful activities. In this way, the origin of illegal funds is hidden by purchasing gold or the gold itself may be stolen or smuggled.

Together with gold, diamonds represent another way to carry on money laundering activities. Indeed, their high intrinsic value and ease trade worldwide make diamonds exposed to their unlawful use as for instance through narcotics trafficking, foreign exchange transactions, fraudulent invoicing and other.

1.3.4.4 Cryptocurrencies

Since its introduction in 2009, bitcoin has been the most emblematic cryptocurrency. Its objective was to create a peer to peer method of payment as an alternative to the commonly used methods and to subtract the monopoly of money creation to Central Banks. In the past ten years, marked by records, hopes, illusions for those who have decided to invest in it, bitcoin has made its contribution to innovation and pushed the world towards virtual money and practices of security and transparency, thanks to the blockchain technology, once unthinkable. Bitcoin was born in a period of financial and banking crisis, a more than favourable period to develop a decentralized system independent from the ones still known. There are three main reasons why bitcoin is likely to be used for money laundering purposes. First of all, the main characteristic of Bitcoin is anonymity: it gives anyone the possibility to transfer small or high sums of money completely anonymously without having to reveal their identity. Second, cryptocurrencies do not undergo to a regulated process of identification of the source of the money as it happens in banks and other financial institutions and each transaction. Third, although being recorded on a blockchain, it is difficultly traceable by authorities.

[22] FATF (2003), "*Report on Money Laundering Typologies 2002-2003"*, pp 19-21

1.4 Money laundering through companies

Nowadays, money laundering increasingly represents a complex process in which different types of crimes, forms and subjects are involved within placement, layering and integrations phases. There are several sectors in which suspicious and fraudulent operations linked to money laundering can occur. In this section, we are going to analyze main techniques and strategies adopted by launderers to bypass the financial system regulation and introduce money with a no legitimate origin across industries.

1.4.1 Smuggling, Casinos and other gambling venues

Cash smuggling, casinos and gambling venues, are the most commonly used companies for the purpose of money laundering[23]. In the first case, smugglers may use bulk or cargo shipments across countries to move large amount of hidden cash inside the goods or even transported by individual couriers who cunningly conceal the its origin and final purpose. Thanks to increased shipping companies and efficiency of several transport systems around the world, movement of cash has been remarkably facilitated creating a wider scenario for money laundering operations.

Casinos and other gambling venues have given rise to increasing money laundering cases through the purchase of chips in the name of a third party or by making the credit available in a casino located in another country. Tokens may also be used for illegal activities as for instance drug and weapons trafficking.

1.4.2 Insurance and Security companies

Within insurance sector, clients of the insurance company buy the insurance policy with an upfront lump sum and later redeem it back at a lower price by paying a fee to the insurance company. This operation allows the launderer to clean the money invested by receiving a check from the insurance company that may also represent a guarantee for any financial loan. Moreover, single premium contracts characterized by fewer liquid transactions and procedures give launderers the opportunity to carry out criminal activities linked to money laundering, thanks to a clear time span in between the crime and the possible payoff.

Criminal operations can take place also in the security sector, especially during the layering and integration phases. In the latter case, securities are purchased with funds coming from unlawful activities and then sold, using these funds as legitimate. It may happen that specific type of

[23] Reuter, P. Truman, E. M. (2004), "*Chasing dirty money, the fight against money laundering, Institute for International Economics"*, pp. 28-29

securities without a registered owner are traded in the market, the European one. It is the case for instance of the bearer securities that are transferred physically and no paper trails are left. In this way, money laundering activities involving securities may be fostered within the market but at the same time many European countries decided to gradually dispose of the bearer securities use accordingly.

Suspicious operations may also result from "put" and "call" transactions which can give the buyer the right to sell and buy a security at the exercise price respectively. But, in this case the client may decide to pay the broker with unlawful funds and get the winning payment back from the broker with clean money[24].

1.4.3 Real estate companies

One of the most sensitive sectors for money laundering and criminal operations in general is the real estate since it has some characteristics that make it attractive for money launderers. First, the market in which real estate companies operate is international and consequently difficultly traceable. Second, substantial changes and fluctuations in property prices with related effects on buyers and sellers make it difficult for authorities to detect off-market transactions. Third, different property markets around the world with local factors affecting their price, the value of rents that affects wealth distribution between landlords and tenants and the overall effects of property prices on the building industry are sources of uncertainty that might be exploited by launderers[25].

We are now going to analyze a series of common techniques used by criminal organizations or subjects to implement illicit activities within the real estate sector.

The first method involves credit and finance companies and can happen in two different ways, namely the Loan-Back Schemes and the Back-to-Back Schemes. In Loan-Back Schemes, "*suspected criminals lend themselves money, creating the appearance that the funds are legitimate and thus are derived from a real business activity*"[26] with the aim to hide both the identity and the relationship between the parties involved in the transaction. In Back-to Back Schemes, the borrower receives the loan upon presenting a collateral to the financial institution. Nonetheless, this collateral does not represent a trustworthy tool for the financial institution lending money since it derives from unlawful activities; moreover, even though the presence of these funds is disclosed on a risk management dossier, its analysis may contain imperfections.

[24] Reuter, P. Truman, E. M. (2004), "*Chasing dirty money, the fight against money laundering, Institute for International Economics"*, pp. 28-29

[25] FATF (2007), "*Money laundering and terrorist financing through the real estate sector"*, pp. 4-5

[26] FATF (2007), "*Money laundering and terrorist financing through the real estate sector"*, page 7

The second method within the real estate sector concerns the role of non-financial professionals in facilitating criminal access to financial institutions and carry out real estate transactions. We are talking about gatekeepers, real estate agents, notaries, registrars and so on. Gatekeepers can take on a relevant role in financial operations such as the opening of a bank account and the eligibility for a loan as well as carrying out different operations on their behalf (e.g. cash depositing and cheques issuing). On the other hand, legal subjects as notaries can assist criminals in the purchase or sell of properties for laundering purposes, since they take on a key role in potentially hiding the real ownership, origin and funds that has been generated from the transaction.

Another method used to obscure the ownership, identity of subjects and origin of funds involved in the real estate transaction is represented by corporate vehicles, meant as legal entities operating in different countries and jurisdictions with a low level of control and supervision. In this case, operations are carried out thanks to the establishment of offshore companies, legal arrangements, shell companies and property management companies. In the first case, legal entities incorporated under a national jurisdiction operate with an organized activity under the jurisdiction of a less restrictive rules country. Legal arrangements (e.g. trusts) are characterized by a lack of transparency in the process of concealing the nature and identity of the real beneficiaries. In the following points we define a few cases of misused trust:

- *"certain trusts may exist without the need for a written document constituting them;*
- *in some types of trust, such as discretionary trusts, the beneficiary may be named or changed at any time, which makes it possible to safeguard the identity of the beneficiary at all times up until the moment the ownership of the assets is transferred;*
- *trusts may be set up to manage a company's shares, and they may make it more difficult to determine the identities of the true beneficiaries of the assets managed by the trusts;*
- *certain legislation may expressly prohibit the freezing, seizure or attachment of assets held in trust"* [27].

As well as offshore companies, there are other companies which have been formed in a country but no activities and assets are registered under its jurisdiction. This is the case of shell companies that may be set up in offshore financial centres or tax heavens aiming to carry out fraudulent operations by hiding the identity of the real owners of the company. In case of property management companies, illegal funds are used to buy a property that is later rented to another person providing a legal source of income apparently. In this way, the launderers have the possibility to mix the rental income and the funds deriving from unlawful activities and

[27] FATF (2007), "*Money laundering and terrorist financing through the real estate sector"*, page 13

obscuring, as a result, the origin of illicit funds.

Another method we are now going to analyse concerns the manipulation of a property appraisal or valuation. In particular, before a purchasing or selling operation, the value of a real estate may be manipulated through an overvaluation or undervaluation. For instance, the company willing to purchase a property may create a new shell company to buy it fictitiously. After the acquisition of the property, money launderers purchasing the property again at a much higher price than the original one; in this way, they put illicit funds into the financial system concealing their origin[28].

Following sales of properties can take place in different transactions by increasing their price step by step. One of the most evident example is linked to the reclassification of land that will be no longer used for agricultural purposes but as a building land, with usual local administrations complicity.

Lastly, bank and financial institution investments in the real estate sector represent another way to use funds for fraudulent operations since the asset side of their balance sheet usually corresponds to mortgage lending transactions through which criminals carry out illicit activities.

1.4.4 Legal professionals

After describing the main important methods adopted in the real estate sector, we can now focus on the role of legal professionals in creating the conditions for mistrustful actions. Another frequent strategy adopted by criminals is the creation of companies and trusts. In the former case, obscuring ownership and retaining control represent the reasons for trust creations as well as red flags for money laundering[29]. Other clear indicators may be a lack of a clear and no legitimate economic reason within the project, different ownership framework and economic interests between the parties and the presence of subjects under investigation for similar crimes. Legal professionals can be involved in the management of companies and trusts making the entity operations transparent and legitimate to the market. At the same time, trustees have to comply with the obligation of "*acquainting themselves with all trust property*" and implementing customer due diligence procedures that include to verify the origin of funds. However, there may be cases in which legal professionals act as trustees and use criminal proceeds to foster laundering operations. Clear evidence of this fact may stand out when legal professionals transfer criminal proceeds into a trust they manage by using a client account or

[28] FATF (2007), "*Money laundering and terrorist financing through the real estate sector"*, page 17

[29] FATF Report (2013), "*Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals"*, page 54

when a legal professional such as a notary incorporate companies and undertake a series of operations to misappropriate the funds unlawfully, acting as an apparent legitimate.

Legal professionals may also hold shares in companies as a nominee in order to allow shareholders to hide their ownership of assets since they actively participate as a vehicle for criminal organizations. Anyway, the possibility for legal professionals to hold shares in entities is not permitted in some countries and as a result acting as a nominee likely represent a clear red flag for illicit activities[30].

Another method used by lawyers or notaries to carry out operations in favour of criminal organizations they are cooperating with is to help their clients in managing affairs and making transactions. One of the most used technique is the opening of a bank account on behalf of clients with the aim to conceal the real owner identity of the account and so that doing illegal business activities. Once the bank account has been created, it could represent a "safe channel" to deposit and transfer criminal proceeds that will be used to finance entities and unlawful organizations.

A clear situation can be described with the following example. We can imagine an individual who decides to set up three companies in which three people has been appointed as legal representatives. Afterwards, three different bank accounts are opened in different countries allowing the individual to mix up his criminal funds with legal funds originating from his companies. Finally, one of the three individuals purchase a real estate obtaining the necessary funds from two others[31].

A legal professional can also be involved in the management of a client general affairs. In this case the role of the legal professional consists of undertaking transactions on his favour and providing assistance in any case the client has difficulty in managing his affairs. However, doubtful situations can arise when a notary, lawyer or legal accountant is not acting on his client's interests but rather on other interests linked to activities outside the object and scope of its profession. In this way, legal professionals promote the interests of criminal organizations and support them through several operations including cash deposits into different bank accounts, the purchase or sell of assets and in general many money management transactions.

1.4.5 Commercial websites

Online websites, purchases and payment methods are nowadays attractive sources and systems

[30] FATF Report (2013), "*Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals"*, page 55-62

[31] FATF Report (2013), "*Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals"*, page 65

for money launderers to carry out criminal operations. With reference to commercial websites for instance there are several categories through which online purchases can be made concerning the subjects involved and the type of transaction. It is the case of customer-to-customer, business-to-customer and business-to-business mediation platforms. Given the huge amount transactions that take place every day online, illicit operations and continuous flows of false information are facilitated worldwide[32].

Moreover, there are many and different suspicious operations taking place in the online world. Commercial transactions involving illegal products or services, apparent trustworthy or unreliable websites and false or suspicious identities can be some mechanisms through which criminals implement unlawful operations online.

Similarly, online payment systems may involve unproper exchange information between commercial partners and the transfer of funds originating from illegal activities or no transparent and justified money transfers.

We are now investigating what are the techniques and fraudulent mechanisms that criminals use to carry out illegal operations through online websites and payment systems. As well as using the online world for committing illegal transactions such as selling drugs, selling counterfeit goods, trafficking weapons, and avoiding in this way tax payments and obligations, criminals can develop and have their own website or even use commodities or securities derivatives as an exchange method. Moreover, another common mechanism used by criminals is to sell fictitious goods which will not deliver once the payment has been received.

It is possible to identify some potential vulnerabilities that can help privates and businesses to detect suspicious and unlawful operations occurring online[33]:

- fictitious sales on commercial websites followed by a real payment but goods are not delivered by the seller;
- the sale of goods has been carried out at an overrated price in several transactions or through several buyers;
- the sale of illegal or counterfeit goods using multiple identities;
- the purchase of goods in a luxury shop with cash followed by an online sell at a lower price;
- the purchase of assets with cash from a third part who held these assets on an online account;

[32] FATF (2008), "*Money Laundering and Terrorist Financing vulnerabilities of commercial websites and internet payment systems"*, page 6

[33] FATF (2008), "*Money Laundering and Terrorist Financing vulnerabilities of commercial websites and internet payment systems"*, pp. 16-20

- purchases of goods using anonymous prepaid cards.

Actually, the above-mentioned points are just a few of the vulnerabilities the online websites and transactions are subject to and, as a result, very different cases can arise through the online world creating the need for more attentive and effective customer due diligence procedures.

1.4.6 Money remittance and currency exchange providers

After a brief description of the money laundering risks linked to the online purchasing and payment systems, we can focus on another suspicious sector for unlawful operations: money remittance and currency exchange providers. Thanks to the globalisation and the development of new technologies, the movement of capitals and the range of financial services across the world have spread out increasingly in the last twenty years. In this context, money launderers have the opportunity to carry out illicit operations by moving quickly a huge amount of money through several channels. According to the definition of the Financial Action Task Force, money remittance and currency exchange services include all those financial institutions implementing the following functions as "*currency dealers/exchangers, money remitters and issuers, sellers and redeemers of stored value and monetary instruments, such as money orders and travellers checks*" [34].

Money remittance and currency exchange services are mainly performed by banks, post offices, travel agencies and foreign exchange houses and centres that must be registered or licensed under the central bank or a governmental authority of the country.

In this sector, there several mechanisms through which money launderers conceal the origin or destination of their funds or simply perform criminal operations by using money remittance and currency exchange services. One of the most common technique is defined as "structuring" and consists of splitting several cash transactions into smaller amount ones avoiding in this way some legal requirements. Considering the number of transactions and the one of money remittance providers within a country, detection of these cases represent a difficult and challenging task for law enforcement agencies, also because transactions usually lack paper trail and certainty about the real existence of the parties involved. Another mechanism for money laundering in this sector is represented by the so-called "money mules", those people who make their bank account available to criminals getting a reward back. The scope of this operation is to hide the origin of money and its real beneficiary. In doing so, many transactions from different people and different time span can be implemented making the connection between subjects involved tricky to find out.

[34] FATF Report (2010), "*Money Laundering through Money Remittance and Currency Exchange Providers"*, page 9

The use of false identities and remittances to high risk countries with low anti-money laundering measures represent other used techniques for money laundering, considering that operations and customers are often occasional and unrelated. In addition, usual cross-countries operations together with the "presence" of false or no-identified people create a complex scenario in which competent authorities (e.g. FIUs or a governmental authority) have to deal with a range of diversified and continuously changing situations.

Another technique to launder money is to get the ownership of the money remittance or currency exchange company, directly or through an agent. In this way, money remitters and currency exchange providers are linked to criminal organizations and can provide services as well as support to them. Proceeds originating from illegal operations can be used to finance the money remittance and currency exchange provider or exchanged in another currency to conceal their origin, make transactions apparently lawful or transfer it in a country with a low-jurisdiction profile.

1.5 Conclusion

In this chapter we first introduced our main discussion topic about money laundering. After a brief description of the phenomenon with its nature and main characteristics according to the Vienna Convention and Palermo Convention, we described the three-step approach through which money laundering operations take place: placement, layering and integration. In the following sections of the chapter we focused on the most common money laundering techniques that criminals use to conceal the origin and destination of their illicit funds. In particular, we described the role of financial institutions, no-bank financial institutions and non-financial businesses as a vehicle for money laundering operations. In this section, we also pointed out other channels through which criminals use their illicit proceed and carry out suspicious operations. It is the case for instance of the electronic funds transfers, the legal sector and the gold and diamond market. Finally, after having described some of the most currently used methods for money laundering, we described this phenomenon under the perspective of a few involved sectors: real estate, legal professional, online websites and payment and remittance and currency exchange providers.

Second Chapter

Money laundering legislation

2.1 Introduction

With respect to money laundering, the European and National legislators committed to implement important measures over the last thirty years with the aim to strictly regulate this phenomenon and most importantly prevent the unlawful use of money for business or criminal activities purposes. In particular, the European Union issued four main directives as regards anti-money laundering:

- the directive 1991/308 of the Council, that first introduced the issue related to the use of money or proceeds coming from illegal activities (traffic of drugs) and was only addressed to the financial sector;
- the directive 2001/97, which extended the field of application of the previous directive with reference to the activities, jobs and related crimes involved in the specific case;
- the directive 2006/70 of the Commission in application of the directive 2005/60 that, compared to the directive 97, introduced additional measures and orders in order to regulate money laundering for terrorism financing and specifically the beginning of special procedures to identify and verify cases and people involved as well as to apply specific provisions according to the gravity of the case;
- the directive 2015/849 that abrogated the directive 60/2005 and 70/2006.

In this chapter we are going to analyse the main important aspects of the directive 2015/849 with the modifications introduced by the Directive 2018/843 and of the Regulation 2015/847. In addition, we are going to focus on Anti-Money Laundering techniques, procedures and indicators to prevent and detect money laundering cases.

2.2 The Directive 2015/849

The directive 2015/849 of the European Parliament and the Council represents the most recent and current legislation in force that regulates and prevents the use of the financial system for money laundering or for the financing of terrorism and other criminal activities.

At the base of the directive there are some important basic points[35]:

- the unlawful flow of money can undermine the stability, entirety and reputation of the financial system and can represent a threat for the EU market as well as for the international economy;
- the free movement of capital and a wide base of financial services offered in the markets foster money launders and financiers to carry out criminal activities resulting in a lack of stability and trust towards financial institutions and intermediaries;
- preventative measures must be taken at international level. All the measures that have been taken at European and national level must be compatible with international measures and initiatives;
- the identification and check of business owners running a legal subject is necessary to guarantee the transparency, accuracy and truthfulness of information concerning business operations, economic and financial trend and relations with stakeholders and as a result prevent cases of money laundering.

The directive is composed of sixty-nine articles that are gathered in seven main sections: general provisions, customer due diligence, beneficial ownership information, obligation of warning, general and statistical data protection and preservation, policies, procedures and supervision, final measures.

2.2.1 General provisions

In the first section, the European legislator identifies the actions that constitute money laundering activities and the subjects of the current directive, legal entities or natural people carrying on their own business. Particularly, according to the article 1 of the Directive 2015/849 of the European Parliament and the Council, the following activities are at the basis of money laundering[36]:

- the modification or transfer of goods coming from criminal and other illegal activities with the aim to hide their origin or helping the subjects in charge to avoid negative legal consequences as a result of their actions;
- the concealment of the origin, ownership, location and movement of goods, knowing that these goods come from illegal activities;

[35] Directive (EU) 2015/849 of the European Parliament and of the Council, pp. 1-2
[36] Directive (EU) 2015/849 of the European Parliament and of the Council, *General Provisions, Subject-matter, scope and definitions*, pp. 11

- the purchase, possession and use of goods coming from a criminal activity or a participation to it;
- the participation to one of the activities indicated above or the cooperation with someone to help and facilitate the implementation of the activity.

The article 1 of the Directive gives also the definition of "terrorism financing", meaning the supply or collection of funds in different ways with the aim to carry out one of the following crimes or terrorist activities regulated by the EU Council Framework decision of June 13, 2002 on the fight against terrorism[37]:

- *murder, bodily injuries, hostage taking, extortion, committing attacks, threat to commit any of the above,* the so-called "objective elements";
- *acts committed with the objective of seriously intimidating a population, destabilising or destroying structures of a country or international organisation or making a government abstain from performing actions,* the so-called "subjective elements";
- *the presence of a structured group of two or more persons, established over a period of time and acting in concert to commit terrorist offences;*
- *preparatory acts linked to terrorist activities including public provocation to commit a terrorist offence, recruitment and training for terrorism and theft, extortion or forgery with the aim of committing terrorist offences;*
- *inciting, aiding or abetting criminal activities linked to terrorism, as well as attempting to commit certain types of offences.*

In this regard, EU member States commit to criminalise people, groups of people and structured organizations that are responsible for the organization and implementation of one of the above-mentioned activities linked to terrorism. Moreover, each EU country establishes jurisdiction over the cases of terrorism when the offences have been carried out in the territory of the State, the offender is a national or a resident in the country or the offence has been carried out to give benefits to a local entity as well as to damage people or institutions based in that country. Finally, each EU country defines the penalties and sanctions according to the type of crime committed and cooperate with the other EU countries to establish the proper jurisdiction to apply when two or more countries are involved in the case.

Within the first section, article 2 defines the entities and the subjects to whom the directive is addressed[38]: credit and financial institutions, natural people and legal entities in the exercise of

[37] EU Act (2002), "*Council Framework Decision of 13 June 2002 on combating terrorism",* art. 1

[38] Directive (EU) 2015/849 of the European Parliament and of the Council, *Subject-matter, scope and definitions*,

their business including auditing firms, financial consultants, solicitors or notaries taking part in any type of operation of their clients (e.g. real estate transactions, purchase and management of bonds and other financial instruments, founding of a company and related operations), estate agents and all the subjects providing gambling services.

In the application of the directive, member states can decide to rule out all the subjects and entities that carry on an exceptional and low risk of laundering financial business conditioned by the following criteria[39]:

- the financial business is limited in terms of duration and operations;
- the financial business is not part of the core business but is directly linked to it;
- the core business is not offered to the whole market but just to the core business customers.

With reference to the points above, member States establish and apply a specific threshold concerning the size of financial business in terms of revenue according to the type of business. This threshold must guarantee that business operations don't represent a way to carry on money laundering or terrorism financing activities. For this reason, member States commit to pay close attention to those financial businesses considered as risky to promote money laundering or terrorism financing activities and, as a result, commit to adopt measures and other forms of control to avoid illegal activities.

Together with the object activities at the base of money laundering and terrorism financing, this first section analyses also the effects that these activities can have on the market, subject and businesses operating within it.

Particularly, the European Commission commits to prepare a report through which identifying and analysing the risks on the EU market originating from money laundering and other unlawful business activities. Within the written relation, the Commission includes the following elements[40]: the most risk exposed market sectors, the risks linked to each market sector and the most common tools criminals use to carry on business activities deriving from money laundering. In addition, the Commission provides the member states with a written relation in order to help them in the identification, management and reduction of money laundering and financing terrorism risky activities. In doing so, the Commission provides also a set of precautionary recommendations allowing the member States to deal with the above-mentioned risks; consequently, each member State implements appropriate measures to identify, evaluate

art. 2

[39] Directive (EU) 2015/849 of the European Parliament and of the Council, *Subject-matter, scope and definitions*, art. 2, comma 3

[40] Directive (EU) 2015/849 of the European Parliament and of the Council, *Risk assessment*, art. 6

and reduce the risks of money laundering and terrorism financing as well as appoint an authority to coordinate different forms of risk reactions at national level.

At the end of the first section, article 9 of the Directive regulates the policy of highly risky countries that lack of clear strategies in their AML/CFT (Anti-Money Laundering and Countering Financing of Terrorism) legislation and represent a threat for the EU financial system. For this reason, the European Commission has the power to adopt delegated acts in accordance with article 64 of this directive as regards[41]:

- the AML/CFT legal and institutional framework of the country (e.g. the possibility to judge the criminal offence of money laundering and terrorism financing, customer due diligence related provisions and obligation to store the documents);
- the powers and duties competent authorities of these countries are responsible for in the fight against money laundering and terrorism financing;
- the effectiveness and validity of the AML/CFT system to contain the phenomenon of money laundering and other illegal offences in this country;

After having described the main important aspects concerning the first section of the European directive, we now focus on the second section about the measures of customer due diligence.

2.2.2 Customer Due Diligence

This section includes articles from 10 to 29 and it is divided in four sub-sections. In the first sub-section about general provisions, article 10 states that anonymous bank account owners or other saving accounts beneficiaries must be subjected to the procedures of customer due diligence[42]. In this regard, member States prohibit financial and credit institutions to keep anonymous bank accounts and any other form of saving; in addition, they ensure the application of proper customer due diligence measures in the following cases: the establishment of a business relation, the implementation of an occasional economic activity whose value is equal or higher than 15 thousands euros or, in case of natural people, equal or higher to 10 thousands euros in one or more operations, the implementation of economic operations whose value is equal or higher than 2 thousands euros for people and entities operating in the business of gambling, a possible case of money laundering or terrorism financing[43].

The following operations are included in the process of customer due diligence by financial

[41] Directive (EU) 2015/849 of the European Parliament and of the Council, *Third-country policy*, art. 9
[42] Directive (EU) 2015/849 of the European Parliament and of the Council, *customer due diligence general provisions*, art. 10
[43] Directive (EU) 2015/849 of the European Parliament and of the Council, customer due diligence general provisions, art. 11

institutions and obliged subjects[44]:

- the identification and check of the clients based on accurate and trustworthy data and information;
- the implementation of specific measures in order to identify and verify the beneficial owner;
- recurring checks on the business trend and in particular to all the operations being concluded during the period to ensure that obliged subjects accurately know the business, identity and other relevant information of his client;
- implement, if necessary, further measures of customer due diligence with reference to their business operations.

In this regard, it is important to underline that member States adopt measures so that financial institutions and obliged subjects can properly implement customer due diligence measures and can prove their effectiveness against money laundering and terrorism financing. Member States also adopt measures to verify the identity of the customer before the business relation starts and establish that any obliged institution or subject who is unable to respect the above-mentioned operations cannot start its business, carry out economic and bank account operations and continue its business.

Legal freelance professionals, notaries, auditors and other legal consultants are exempted from the application of the above-mentioned measures just in case these subjects have analysed the legal status of their client or act in the name of and on behalf of their client in a legal process[45].

With reference to the risk of money laundering and terrorism financing, member States allow financial institutions or obliged sector to apply basic or more restrictive customer due diligence measures according to the type of business and its risk. In evaluating this aspect, member States and obliged subjects have to take into account the nature and size of business, the type of goods and services sold, the geographical areas of operation, type and origin of the clients and all the suspicious by using a risk-based approach.

As a result, business activities with a higher risk are applied more restrictive measures while lower risk business activities are applied less restrictive ones[46].

Ultimately, the directive gives the possibility to rely on third subjects to fulfil the obligation of customer due diligence in accordance with the above-mentioned activities ruled by article 13.

[44] Directive (EU) 2015/849 of the European Parliament and of the Council, customer due diligence general provisions, art. 13

[45]Directive (EU) 2015/849 of the European Parliament and of the Council, *customer due diligence general provisions*, art. 14, comma 4

[46] Directive (EU) 2015/849 of the European Parliament and of the Council, *simplified customer due diligence*, art. 15

However, obliged subjects are fully in charge to fulfil the final obligation[47]. All the obliged subjects and institutions listed in article 2 and other organizations and institutions established in a member State or in a third country commit to adopt all customer due diligence and record-keeping requirements and they are subjected to supervision procedures with reference to the fulfilment of the obligations regulated by this directive. In addition, obliged sectors cannot rely on third subject who are located in high risk countries. Overall, member States commit so that obliged subjects receive all the information about their obligations of customer due diligence from third entities and subjects.

2.2.3 Beneficial Ownership Information

Section 3 of the Directive analyses the topic of the information about beneficial owners. In particular, companies and all legal entities commit to store and make available all the information and documents about their business; all these information have to be stored in a central register in each member State, for example at the registration office or in a public register and must be accurate and updated. Member States commit so that all the information about real owners are available to the competent authorities, obliged sectors in the framework of proper check of the clients and finally to each stakeholder dealing with these subjects[48]. In this sense, the central register guarantees a no-limit and prompt access to the competent authorities and all the obliged subjects. Moreover, member States establish that subjects relying on nationally regulated trustees have to receive and properly store accurate and updated information about the real ownership of the trustees. In particular, this information includes[49]:

- the identity of the subject establishing the trust relationship;
- the identity of the trustee;
- the identity of the beneficiaries;
- the identity of the people implementing a direct control on the trust.

The trustee has to provide all the above-mentioned information when he establishes a business relation or carries out an occasional economic activity in accordance with article 11 of the present directive. As described in the first part of this section, all the information must be stored in a public register (registration office) that guarantees a no-limit and timely access to the competent authorities and all the obliged subjects in accordance with customer due diligence

[47] Directive (EU) 2015/849 of the European Parliament and of the Council, *performance by third parties*, art. 25
[48] Directive (EU) 2015/849 of the European Parliament and of the Council, *Beneficial ownership information*, art. 30
[49] Directive (EU) 2015/849 of the European Parliament and of the Council, *Beneficial ownership information*, art. 31

provisions.

2.2.4 Reporting obligations

In the fourth section, the directive analyses the reporting obligation. The first subsection introduces the general provisions about this topic. Specifically, article 32[50] states that "*each member States establishes a FIU (Financial Intelligence Unit) to prevent, detect and fighting against money laundering and financing of terrorism*". According to the definition of the European Commission[51], the FIU is "*a central, national unit that is responsible for receiving and analysing information from private entities on financial transactions which are considered to be linked to money laundering and terrorist financing*".

The European Commission is notified the name and address of each financial intelligence unit by the member States. Each FIN is autonomous and independent from the others, so it has the power to carry out its functions without limitations, including the analysis, request and dissemination of specific information. In addition, being a national central unit, it has the responsibility to receive and analyse suspicious information about money laundering operations and terrorism financing activities. Consequently, each FIU has to notify the results of its analyses with the competent authorities whenever there are suspicious reasons for the above-mentioned activities.

Each financial intelligence unit is provided with proper financial, human and technical resources in order to fulfil their tasks. In doing so, the FIUs have a direct or indirect access to a wide base of information necessary to fulfil their tasks accurately. In any case financial intelligence units receive a request of information which is motivated by the risk of money laundering, terrorism financing activities and related offences, each FIU is in charge of responding to the request of information by the competent authorities of each member State; later, competent authorities commit to give a feedback to the FIUs about the use of information and the results of the investigations.

When there is a suspicious operation linked to a money laundering or terrorism financing activity, member States give the FIU of each country the power to act immediately by suspending, analysing and confirming the offensive activity and sharing the results of the investigation to the competent authorities.

The function of each FIU is carried out as follows[52]:

[50] Directive (EU) 2015/849 of the European Parliament and of the Council, *reporting obligation, general provisions*, art. 32

[51] Official website of the European Union, Migration and Home Affairs, *definition of Financial Intelligence Unit (FIU)*, https://ec.europa.eu/home-affairs/e-library/glossary/financial-intelligence-unit-fiu-0_en

[52] Directive (EU) 2015/849 of the European Parliament and of the Council, reporting obligation, general

- an analysis focused on selected information, individual cases and specific objectives, considering the type and quality of received information;
- a strategic analysis aimed at identifying money laundering and terrorism financing trends and models.

It's important to underline that obliged sectors and institutions, including also their directors and employees, commit to inform and collaborate with the FIU when there is a concrete and reasonable ground to suspect that profits are originated from money laundering activities of financing of terrorism operations; moreover, they commit to provide all the required information in accordance with the current legislation[53]. When member States suspect that a specific operation is linked to criminal activities or financing of the terrorism, obliged subjects are prohibited to carry on this kind of operation as long as they comply with the necessary procedures and instructions in accordance with article 33 or other instructions from the financial intelligence unit.

Article 39 regulates the prohibition for obliged subjects and entities to disclose the information included in article 33 to their customers and third parties; this prohibition does not include the disclosure to the competent authorities (e.g. self-regulatory bodies). The disclosure among financial institutions and credit institutions as well as among them and their majority-owned subsidiaries and branches is allowed as long as they comply with the group policies and procedures[54].

2.2.5 Data protection, record-retention and statistical data

The fifth section of the Directive analyses the topics of data protection, record retention and statistical data. Article 40 establishes that obliged subjects and entities are required to keep all the information and documents indicated below in accordance with the national law with the aim to prevent and avoid any possible case of money laundering or financing of terrorism. Specifically, the following information must be carefully stored[55]:

- a copy of the documents and information in compliance with customer due diligence requirements listed in paragraph 2.2.3 for a five-years period following the end of a business relation or an occasional transaction;

provisions, art. 32, comma 8

[53] Directive (EU) 2015/849 of the European Parliament and of the Council, *reporting obligation, general provisions*, art. 33

[54] Directive (EU) 2015/849 of the European Parliament and of the Council, *reporting obligation, prohibition of disclosure*, art. 39

[55] Directive (EU) 2015/849 of the European Parliament and of the Council, data protection, record retention and statistical data, art. 40

- the transactions recording resulting from both original and copies of documents that are accepted in judicial proceedings for a five-years period following the end of a business relation or an occasional transaction.

After the period of five years, obliged subjects commit to delete personal data, unless other provisions set by the national law. In this case, member States can allow a longer period of information and data retention after an accurate assessment of the necessity of the case and considering its importance in preventing and detecting any possible money laundering and terrorism financing operation.

In accordance with the current directive, personal data use and processing is only justified by the purpose of preventing money laundering and terrorism financing activities and, as a result, the use and processing of data for any other purpose is prohibited[56].

Moreover, obliged subjects are required from member States to arrange systems that allow them to promptly and effectively respond to any enquiry from the financial intelligence unit (FIU), according to their national law, with the aim to verify if they have maintained a five-years business relation with a specific person.

With the aim to contribute to the preparation of the risk assessment report, member States ensure their capability to assess the effectiveness of anti-money laundering systems by generating statistical data on matters relevant to the effectiveness of such system[57].

2.2.6 Policies, procedures and supervision

Second to last section describes the topic of policies, procedures and supervision of the obliged subjects. This section comprises 18 articles divided in 4 sub-sections: internal procedures, training and feedback (1st sub-section), supervision (2nd sub-section), cooperation (3rd sub-section) and sanctions (4th directive).

Article 45 widely describes the obligation for any obliged subject to comply with the provisions, policies and procedures at group level or in case of branches and/or majority-owned subsidiaries located within the European Union or in a third country with the aim to effectively deal with the risk of money laundering and financing of the terrorism[58].

Specifically, obliged subjects and entities which are part of a group are required to carry out policies and procedures at group level, including policies and procedures for sharing

[56] Directive (EU) 2015/849 of the European Parliament and of the Council, *data protection, record retention and statistical data*, art. 41

[57] Directive (EU) 2015/849 of the European Parliament and of the Council, *data protection, record retention and statistical data*, art. 44

[58] Directive (EU) 2015/849 of the European Parliament and of the Council, *policies, procedures and supervision, internal procedures, training and feedback*, art. 45

information about anti-money laundering and terrorism financing activities and data protection within the group. In case obliged subjects have branches or majority-owned subsidiaries in another member State or in a third country, these entities have to fulfil the obligations according to the provisions of the member State or third country in which they are located. Whether a third country jurisdiction does not enable the implementation of policies in the country, branches and majority-owned subsidiaries established within this country commit to implement additional policies in order to effectively deal with the risk of money laundering and terrorism financing as well as informing the competent authorities of the country[59].

It's important to highlight that obliged subjects are required to implement measures in proportion to the size, nature and risks of their business; these measures are also addressed to their employees and include their participation to training programmes allowing them to recognise risky operations linked to money laundering and financing of terrorism and adopt specific actions accordingly. For this reason, member States allow obliged subjects to have access to relevant and up-dated information about procedures and actions implemented by any subject responsible for money laundering and/or financing the terrorism and recognise possible suspicious operations[60].

In the second sub-section, the directive regulates the obligation of supervision within the power of competent authorities. Indeed, they are in charge of implementing measures in order to verify the respect of this directive. In doing so, member States manage to provide them proper powers and a set of resources (human, financial and technical) to perform their functions; competent authorities have also stronger supervisory powers as regards financial and credit institutions and gambling services providers[61].

Furthermore, in applying a risk-based approach on supervision, member States assure that competent authorities[62]:

- have a clear overview and understand the risks of money laundering and terrorism financing in their country;
- have a no-limit access to all important information concerning national and international risks linked to goods, services and clients of obliged sectors;

[59] Directive (EU) 2015/849 of the European Parliament and of the Council, *policies, procedures and supervision, internal procedures, training and feedback*, art. 45, comma 5

[60] Directive (EU) 2015/849 of the European Parliament and of the Council, policies, *procedures and supervision, internal procedures, training and feedback*, art. 46

[61] Directive (EU) 2015/849 of the European Parliament and of the Council, *policies, procedures and supervision, supervision*, art. 47-48

[62] Directive (EU) 2015/849 of the European Parliament and of the Council, *policies, procedures and supervision, supervision*, art. 48, comma 6

- adapt the intensity of supervision considering the profile of risks of obliged subjects and the risks of money laundering and terrorism financing in the country.

Competent authorities carry out a risk assessment of obliged entities periodically and in any case relevant events or changes in their organization and management occur.
Finally, this subsection states that some specific subjects including for instance currency exchange or trust company providers have to get a license or providers or gambling services have to be regulated[63].

The third sub-section describes how cooperation between competent authorities takes place, both at national and European level. Particularly, art. 49 gives a brief description about national cooperation and states that all authorities operating in AML/CFT activities, including policy makers, financial intelligence units, supervisors and all other competent authorities are provided with effective tools and mechanisms that allow them to collaborate through the implementation of policies to hinder money laundering and terrorism financing[64].
At European level, the commission supports the competent authorities to facilitate the coordination between competent authorities including periodical arrangements of meetings between the representatives of Member States' FIUs in order to foster cooperation between them and as a result the exchange of opinions and information on most relevant topics (e.g. effective cooperation among the FIUs and identification of risky operations of money laundering and financing of terrorism). When a financial intelligence unit of a member State receives a report about a suspicious and risky operation of money laundering and financing of terrorism in another member State, it provides it to the FIU of that member State promptly. Consequently, this financial intelligence unit will commit to use all the available national powers to get and analyse this information, when the request of information is compatible with the type of suspicious activity or operation. In case a FIU needs to get addition information from an obliged subject operating within the State but located in another member State, the request will be addressed to the financial intelligence unit of the member State where the obliged entity is located. Any FIU can reject to provide and exchange information only in specific and unusual circumstances when the exchange is not legally consistent with its national legislation; in this regard, it's important to specify the cases in which the exchange is not allowed in order to avoid unfair limitations to the free exchange of information. Furthermore,

[63] Directive (EU) 2015/849 of the European Parliament and of the Council, *policies, procedures and supervision, supervision*, art. 48, comma 7
[64] Directive (EU) 2015/849 of the European Parliament and of the Council, *policies, procedures and supervision, national cooperation*, art. 49

all this information must be used by each financial intelligence unit to fulfil their tasks in accordance with the measures of this directive[65].

Finally, the exchange of information between FIUs must be implemented by using safe and protected channels of communication as well as by technology-advanced supporting systems that allow each FIU to match data and information with other FIUs and exchange confidential information safely.

The last sub-section of the main section concerning policies, procedures and supervision operations implemented by obliged subjects is about sanctions.

In general, article 58 of the Directive states[66] that "*Member States shall ensure that obliged entities can be held liable for breaches of national provisions transposing this Directive in accordance with this Article and Articles 59 to 61; any resulting sanction or measure shall be effective, proportionate and dissuasive.*

In this regard, each member State defines the regulation to be applicable and related sanctions in order to allow competent authorities of each member State to apply the sanctions in violation and in accordance with this Directive. In case the national legislation of a member State has already defined criminal sanctions for some breaches, that member State can decide not to lay down further rules for administrative measures and sanctions. When breaches of national provisions involve legal entities, measures and sanctions will be applied to their management body or other physical people in charge of the breach[67].

Competent authorities of each member States have the power to impose measures and sanctions in accordance with the national law and this directive in different ways[68]: directly to the subject or legal entities that violated the law, cooperating with other authorities within the country or located in EU area, being delegated by other authorities responsible for applying the law and imposing the sanction and finally relying on competent judicial authorities. Moreover, competent authorities commit to actively cooperate each other in order to ensure the achievement of the expected results thanks to the application of the law and respective sanctions.

Most importantly, article 59 states that member States ensure the application of this article to all obliged subjects responsible for the breach of measures included in the topics concerning

[65] Directive (EU) 2015/849 of the European Parliament and of the Council, *policies, procedures and supervision, cooperation between FIUs and with the Commission*, art. 51-53

[66] Directive (EU) 2015/849 of the European Parliament and of the Council, *policies, procedures and supervision, sanctions*, art. 58

[67] Directive (EU) 2015/849 of the European Parliament and of the Council, *policies, procedures and supervision, sanctions*, art. 58, comma 2-3

[68] Directive (EU) 2015/849 of the European Parliament and of the Council, *policies, procedures and supervision, sanctions*, art. 58, comma 5

customer due diligence, suspicious transaction reporting, record-keeping and internal controls. In any case, administrative measures and sanctions towards obliged subjects have to be followed by[69]:

- a clear identification of the subject or entity responsible for the breach through a public statement;
- the obligation for the subject involved in the breach to interrupt its conduct;
- a temporary ban for managers or people carrying out managerial activities within an obliged entity;
- a maximum amount of the sanction that must be at least twice the amount of the proceeds resulting from the violation;

Once the person in charge of the breach has been identified, the nature of the crime has been defined and the type and amount of the sanction has been set out, the competent authorities commit to publish the decisions on their website. In determining the type and the level of the sanction, the competent authorities have to consider some important aspects including for instance the duration and gravity of the breach, the degree of responsibility of the person involved, the benefits resulting from the breach for the person in charge and the presence of previous breaches by the same person[70].

2.2.7 Final provisions

The last part of the directive is about final provisions. The first comma of article 64 states[71] that "*The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article* and the Commission has to notify it to the European Parliament and the Council.

Previous EU directives 2005/60 and 2006/70 have been repealed from the date this directive entered into force and all the member States commit to implement all the measures, administrative procedures and laws in order to harmonise their legislation with the one of the European Union, within a two-years' time period.

In our case, Italy accepted and complied with the provisions included in the directive 2015/849 by adopting the Legislative Decree 2017/90 we will discuss later on.

[69] Directive (EU) 2015/849 of the European Parliament and of the Council, *policies, procedures and supervision, sanctions*, art. 59

[70] Directive (EU) 2015/849 of the European Parliament and of the Council, *policies, procedures and supervision, sanctions*, art. 60

[71] Directive (EU) 2015/849 of the European Parliament and of the Council, *policies, procedures and supervision, final provisions*

2.3 Directive 2018/843

In 2018, the European Parliament and the Council jointly introduced a new directive (2018/843) within the topic of Anti Money Laundering and Combating the Financing of Terrorism (AML/CFT). This directive became the fifth one that has been implemented over the last thirty years, after the first four directives (1991, 2001, 2005 and 2015) and has introduced important modifications and integrations to directive 2015/849 in order to strengthen the provisions laid down in the previous one and above all to defend the financial system and prevent unlawful operations in the field of terrorism financing and money laundering. Indeed, the main goal of the directive is to guarantee a higher transparency of financial operations, legal entities and financial institutions through the adoption of effective measures to improve the current framework of prevention and limit illegal operations and in general the financing of terrorism[72]. The most relevant topics the directive has focused on are currency exchange services between virtual currencies and legal currencies and the lenders of digital portfolio services, prepaid cards, the financial intelligence units (FIU), trust and similar institutions.

2.3.1 Currency exchange transactions

In the first case, it's interesting to notice how all the subjects involved in currency exchange transactions and services were not obliged to detect and report suspicious operations of money laundering and terrorism financing according to the previous directive. But, at the same time, increasing cases of hidden transactions between currencies and their unlawful use for criminal purposes have created negative effects for the financial system and the subjects operating within it, fostering the EU legislator to modify the directive 2015/849 and included lenders of virtual currency transactions and services within the group of obliged subjects[73].

2.3.2 Prepaid cards

Prepaid cards are another instrument widely used in the market to facilitate money transfers but also transactions aiming at finance the terrorism and related operations; indeed, prepaid cards usually have low imports and are not subject to traceability. As a result, it became necessary to reduce the threshold under which obliged subjects can avoid implementing specific measures of customer due diligence according to the directive[74].

[72] Directive (EU) 2018/843 of the European Parliament and of the Council, *Amendments to directive 2015/849*
[73] Directive (EU) 2018/843 of the European Parliament and of the Council, *Amendments to directive 2015/849*, art. 1
[74] Directive (EU) 2018/843 of the European Parliament and of the Council, *Amendments to directive 2015/849*, art.12

2.3.3 The role of Financial Intelligence Unit

Another important aspect the directive has focused on concerns the role of FIUs. Indeed, financial intelligence units exercise one of the most essential role in the system to deal with risky and suspicious operations linked to money laundering and financing of terrorism. In this sense, they have the function and the responsibility to autonomously receive, analyse and detect information about possible operations about money laundering and terrorism financing. However, the lack of a common regulation at international level and differences between FIUs within the EU in terms of powers, functions and competencies make difficult the implementation of a common and coordinated approach in the process of investigation of causes related to terrorism[75].

2.3.4 The role of trust and similar institutions

Finally, the directive has focused on the regulation of trust and similar legal entities. According to article 2 of the AIA Convention of 1985[76], the trust can be defined as a "*legal relationship created – inter vivos or on death – by a person, the settlor, when assets have been placed under the control of a trustee for the benefit of a beneficiary or for a specified purpose".* As it is stated from the definition, the trust involves three subjects:

- the settlor is the person or legal entity who establishes the trust and gives the trustee the full availability of its assets;
- the trustee is the person or legal entity who receives and control the assets of the settlor for the benefit of a beneficiary;
- the beneficiary is the final person or legal entity who has a strong interest in the assets of the settlor;

This relation between the settlor, trustee and beneficiary shows other important characteristics according to article 2:

- *the assets constitute a separate fund and are not a part of the trustee's own estate;*
- *title to the trust assets stands in the name of the trustee or in the name of another person on behalf of the trustee:*

[75] Directive (EU) 2018/843 of the European Parliament and of the Council. *Amendments to directive 2015/849*, Art. 30

[76] AIA Convention (1985), *Law applicable to trusts and on their recognition*, art. 2

- *the trustee has the power and the duty, in respect of which he is accountable, to manage, employ or dispose of the assets in accordance with the terms of the trust and the special duties imposed upon him by law*.

In this three-side relation the trustee is the only person in charge in dealing with third parties, since the trust is not an autonomous legal subject; consequently, the trust is just established and makes available an amount of capital that must be used for a specific purpose. Furthermore, the legal system applied to trust and similar legal entities should be comparable to the legal system of companies and other legal entities as regards the set of information about their beneficial ownership. The domestic legislation of each member State should also avoid that trust and other similar legal entities use the financial system to implement money laundering or terrorism financing operations. But, at the same time, different legislations within the European Union between member States make difficult the implementation of supervision procedures of these entities.

2.4 Main modification of the Directive 2018/843

In this context, directive 2018/843 introduced important modifications to the previous directive in order to go over the issue of asymmetric legislation among countries and strengthen cooperation between financial institutions to hinder criminal and other unlawful activities.
The first important modification concerns the list of subjects or entities obliged to comply with anti-laundering measures. Indeed, the list now includes providers of currency exchange services between legal and virtual currency, providers of digital portfolio services, people or intermediaries trading artworks and those working in auction houses[77].
With reference to the customer due diligence section, the directive introduced further instruments enabling credit and financial institutions to identify and verify their customers[78]:

- electronic identification systems, trust services[79] and any other electronic system regulated and accepted by national authorities;
- when the identified owner is a senior manager, obliged subjects commit to adopt all the necessary measures to verify his identity and keep stored the records of the measures taken;

[77] Directive (EU) 2018/843 of the European Parliament and of the Council, *Amendments to directive 2015/849,* art. 1
[78] Directive (EU) 2018/843 of the European Parliament and of the Council, *Amendments to directive 2015/849,* art. 13
[79] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services

- when a business relationship with a company, legal entity, trust or any other legal organisation has been established, obliged subjects collect the proof of the registration;
- stronger customer due diligence measures for those business relationship or operations involving higher risks countries.

The fifth directive introduced relevant modification to the section about the information of beneficial ownership. Indeed, article 30 of the previous directive has been modified by setting out that the information held in a public register are accessible to beneficial legitimate people but also to the general public. As a result, according to the fifth comma of article 30, information about beneficial ownership are accessible to: competent authorities and financial intelligence units, obliged entities in accordance with the framework of customer due diligence set out in the second section and any natural person[80]. The first comma of new article 32[81] bis states that competent authorities and FIUs can have access to a wide set of information not only about legal entities but also about all the citizens of the European Union. Particularly, central registers or electronic data systems allow the identification of any natural person or legal entity who holds or controls payment and bank accounts identified by an IBAN as well as safe-deposit boxes held by a credit institution within their territory. Finally, new article 32 ter states that FIUs and competent authorities can have access to all the information that allow a prompt identification of any natural or legal persons owning real estate, through register or electronic data retrieval systems when available.

2.5 Regulation 2015/847

Together with directive 2015/849, the European Parliament and the Council adopted the regulation 2015/847 which represents another important European source of law within the topic of AML/CFT. Differently from the directives, EU regulations are directly applicable on each member State that receives and accepts it without issuing a specific national law to comply with it.

This regulation repealed the previous regulation 2006/1871 and particular regulates the information about payers and payees accompanying transfers of funds with the aim to prevent, detect and investigate possible cases of money laundering and terrorism financing.

[80] Directive (EU) 2018/843 of the European Parliament and of the Council, *Amendments to directive 2015/849*, art. 30

[81] Directive (EU) 2018/843 of the European Parliament and of the Council, *Amendments to directive 2015/849*, art. 32

2.5.1 Subject matter, scope and definition

Article 2 defines the operations and transfers to which the regulation is applied. The definition of the first comma of art. 2[82] states that "*This Regulation shall apply to transfers of funds, in any currency, which are sent or received by a payment service provider or an intermediary payment service provider established in the Union"*. Consequently, this regulation does not apply to the transfer of funds following payments made with credit cards, electronic money instrument, mobile phones and any other electronic device with similar characteristics, when all these methods are used to carry out a person to person transfer of funds. This regulation does not apply to all those money transfer operations in which[83]:

- the payer has to withdraw cash from his/her own payment account;
- there is a transfer of funds to a public authority (e.g. tax payment);
- both subjects, the payer and payee, are payment service providers operating on their behalf;
- exchange of cheque images has been carried out through.

2.5.2 Obligation on payment service providers

Article 4 describes all the information accompanying transfers of funds within the section concerning the obligations on service providers. Specifically, transfer of funds from the payer to the payee has to be accompany by some specific information of the payer including the name, the payment account number, the address, an official document with the number and his customer identification number. On the other hand, transfer of funds has to be accompanied also by information of the payee including his name and payment account number[84]. In both sides, payment service provider guarantees that the transfer of funds is accompanied by the above-mentioned information. The disclosure of payment account numbers of both parties is necessary in case all the payment service providers involved in the payment chain are located within the EU territory. Otherwise, when payment service providers are located outside the EU territory and the payment comes from a unique payer, article 4 does not apply as long as all the information of article 4 are contained in the batch file transfer.

In the transfer of funds transaction, the payment service provider of the payee has some obligations. The first one is to detect missing information on the payer or the payee by implementing effective procedures to verify that all the required identity and payment

[82] Regulation (EU) 2015/847 of the European Parliament and of the Council, *scope*, art. 2
[83] Regulation (EU) 2015/847 of the European Parliament and of the Council, *scope*, art. 2, comma 4
[84] Regulation (EU) 2015/847 of the European Parliament and of the Council, *obligation on payment service providers, information accompanying transfers of funds*, art. 4

information and data have been properly disclosed throughout the payment process in accordance with the provisions laid down in this regulation[85].

When the transfer of funds is accompanied by missing or incomplete information by the payer, the payment service provider of the payee has to apply specific and consistent risk-based procedures in order to understand if the transfer of funds could be carried out, rejected or suspended. As a result, when information and data are incomplete or do not comply with the measures set out in this regulation, the payment service provider can ask for the missing information to the payer involved in the transaction or can reject the transfer. Only after required information have been provided and once verified their correctness and validity, the payment service provider of the payee will authorise the transaction and the credit in the payee's payment account. On the contrary, when the payment service provider of the payer does not provide or constantly denies to provide the required information, the payment service provider of the payee may take measures, as setting specific warnings or deadlines by the time it rejects future transactions and money transfers from that service payment provider. Finally, the payment service provider takes into consideration the missing and uncomplete information to assess if the transfer of funds is suspicious and shall be reported to the Financial Intelligence Unit (FIU)[86].

When a transfer of funds involves an intermediary, all the obligations about missing or uncomplete information we have just described applies to the intermediary as well.

2.5.3 Information, data protection and record-retention

Section 3 of this regulation analyses the topic concerning information, data protection and retention. With reference to the provision of information, article 14[87] states that "*payment service providers shall respond fully and without delay and in accordance with the procedural requirements laid down in the national law of the Member State in which they are established, to enquiries exclusively from the authorities responsible for preventing and combating money laundering or terrorist financing of that Member State concerning the information required under this Regulation"*. As a result, payment service providers are responsible to quickly and exclusively respond to the enquiries from the competent authorities of the country in which they are established in accordance with the provisions and laws of that member State.

[85] Regulation (EU) 2015/847 of the European Parliament and of the Council, *obligation on payment service providers, detection of missing information on the payer or the payee*, art. 7

[86] Regulation (EU) 2015/847 of the European Parliament and of the Council, *obligation on payment service providers, Transfers of funds with missing or incomplete information on the payer or the payee*, art. 8-9

[87] Regulation (EU) 2015/847 of the European Parliament and of the Council, information, *data protection and record-retention, provision of information*, art. 14

Furthermore, payment service providers must respect and process informative data in accordance with the provisions laid down in this Regulation and information must be only used for the purpose of preventing money laundering and terrorism financing. All data have to be stored for a period of five years, unless otherwise set out by the national legislation of a member State that can authorise a longer period after verifying the reasons and necessity of this further retention[88].

With reference to the violation of specific rules laid down in this Regulation, member States set out administrative measures and sanctions and ensure that they are implemented. In accordance with directive 2015/849, measures and sanctions must be proportionate, effective and dissuasive. The first comma of article 17 states another important aspect about the implementation of measures and sanctions within the EU. Indeed, when a member State sets out criminal sanctions in violation of this Regulation, it may decide not to lay down further measures and sanctions since the domestic legislation of that member State has already defined the jurisdiction to be implemented. In this case, the European Commission has to be notified with the criminal provisions set out by that member State[89].

Competent authorities of each member State are endowed with supervisory and investigating powers necessary to exercise their functions. Moreover, in the implementation of specific measures and sanctions, competent authorities cooperate each other for the purpose of ensuring the achievement of the desired results and dealing with cross-border cases.

As laid down in the directive 2015/849, the imposition of administrative measures and sanctions by the competent authorities can be made: directly to the subject or legal entities that violated the law, cooperating with other authorities within the country or located in EU area, being delegated by other authorities responsible for applying the law and imposing the sanction and finally relying on competent judicial authorities.

The monitoring and reporting of breaches are also facilitated by effective instruments and procedures established by each member State in order to ensure the respect of the provisions laid down in this Regulation[90].

The last part of the Regulation describes the role of the Committee on the prevention of money laundering and terrorism financing in assisting the Commission as regards implementing powers, the derogations to this Regulation (specifically about agreements with countries and territories which do not form part of the territory of the Union) and the final provisions.

[88] Regulation (EU) 2015/847 of the European Parliament and of the Council, *information, data protection and record-retention*, art. 16

[89] Regulation (EU) 2015/847 of the European Parliament and of the Council, *sanctions and monitoring*, art. 17

[90] Regulation (EU) 2015/847 of the European Parliament and of the Council, sanctions and monitoring, art. 21

2.6 AML techniques

According to the World Bank definition[91], money laundering can be defined as "*the process by which proceeds from a criminal activity are disguised to conceal their illicit origins.* As laid down in the EU Directive 2015/849, money laundering process can be implemented in different ways. Most important money laundering activities include for instance the transfer or modification of some goods with the scope to hide their origin and the concealment of their origin, location and movement, knowing that these goods come from criminal or other unlawful activities. As well as money laundering activities, there is another common phenomenon that undermines the stability, integrity and functioning of the financial system and create negative economic effects on financial institutions, legal entities and on the economy of the countries involved. This is the phenomenon of the terrorism financing[92], basically defined as "*the financial support, in any form, of terrorism or of those who encourage, plan, or engage in terrorism"*. As a result, money laundering and terrorism financing represent a double mechanism to hide the illegal origin of financial proceeds that will be used later on to start a new business, carry on other economic activities or even other unlawful operations.

In this section we are going to briefly describe what are the main anti-money laundering (AML) measures and techniques that are implemented by financial and credit institutions, legal entities, counsellors, auditors and other legal professionals to detect and identify money laundering operations efficiently.

2.6.1 Customer identification and due diligence procedures

One of the most important requirements for financial institutions operating within the European Union is to have adequate customer identification and due diligence procedures to identify and check out the correctness and truthfulness of personal and financial information provided during this phase[93]. In this way, financial institutions can have a clear knowledge about their customers preventing possible cases of money laundering and giving benefits to the financial system as a whole. Consequently, implementing appropriate customer identification and due diligence procedures can result in positive effects for both the whole economic-financial system and the involving entities as[94]:

---

[91] World Bank (2006)*, "Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism (second edition)"*, page 19

[92] World Bank (2006), "*Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism (second edition)"*, page 19

[93] World Bank (2006), "*Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, preventive measures, customer identification and due diligence"*, page 99

[94] World Bank (2006), "*Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, preventive measures, customer identification and due diligence"*, page 101

- the promotion and improvement of good business, governance, and risk management among financial institutions;
- the maintenance of the financial system integrity enabling also the development efforts in emerging markets;
- the reduction of fraud and other financial crimes incidence;
- the protection of the financial organization reputation against damaging effects of association with criminals.

However, different kind of transactions and customers imply a different risk-based approach accordingly. Indeed, lower-risk customers and operations imply the application of simplified measures and procedures while, on the other hand, enhanced and stricter measures are required for higher-risk customers and transactions. In this latter case, it is possible to identify specific circumstances in which the implementation of enhanced due diligence measures is required. According to the World Bank discussion about this topic, we can mention[95]:

- Politically Exposed Persons (PEPs) that include only those people taking up public functions in a foreign country (e.g. Head of the State or of the Government);
- Cross-Border Correspondent Banking Relationships which may represent a way for large entities to open up to financial markets and avoid the implementation of appropriate due diligence procedures, considering the low level of arrangements required in their country;
- Non-Face-to-Face Customers, considering that many operations and services are implemented by customers virtually;
- Introduced Business, meant as those financial businesses that have "introduced customers" by intermediaries and to whom due diligence measures have not been carried out;
- Other High-Risk Business, including uncommon large operations that have not a specific economic and lawful purpose and all those suspicious transactions with countries not complying with the FATF (Financial Action Task Force) recommendations.

2.6.2 Record keeping requirements and suspicious transaction reporting

Another important measure consists of keeping customer identity and transaction records for a period of at least five years. In this way, financial institutions can prevent and detect money

[95] World Bank (2006), "*Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, preventive measures, customer identification and due diligence"*, pp. 106-109

laundering and financing of terrorism connected operations. In some specific cases, financial institutions are required to keep identity and transaction detailed records for a longer period than five years, according to the type of business and its regulation. It may be the case for instance of insurance and security sectors[96].

Whenever financial institutions have the suspect that a transaction is linked to money laundering or proceeds derive from illegal operations, they have to report it to the competent authorities. Any complex transactions as well as any transaction missing a clear economic and lawful purpose is considered suspicious and consequently further investigations are necessary to identify and detect its nature[97].

Moreover, financial institutions of each country may require a cash reporting when the transaction exceeds a fixed threshold. This threshold may be set out according to the national jurisdiction or a specific regulation by the government supervisory agency. Cash transactions reporting also apply to multiple cash transactions when consolidated operation exceeds the threshold, cross-border movement of cash and modern money management techniques (e.g. direct deposit, debit and credit cards and book-keeping record of securities)[98].

2.6.3 Internal controls, compliance and audit

Another important aspect about financial institutions concerns the establishment and conservation of internal policies and procedures to prevent and avoid transactions linked to money laundering and financing of terrorism purposes (e.g. internal employees training). Other forms of internal control and compliance may be the establishment of an AML/CFT administration office and a separate audit function within each financial institution.

Overall, in dealing with the prevention and detection of money laundering and terrorism financing operations, national authorities commit to verify and ensure the implementation of the above-mentioned measures by financial institutions setting out specific requirements and provisions[99].

2.6.4 Functions of the FIU

In the process of fighting against money laundering and terrorism financing a very important

[96] World Bank (2006), "*Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, preventive measures, record keeping requirements"*, page 114

[97] World Bank (2006), "*Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, preventive measures, suspicious transactions reporting"*, page 116

[98] World Bank (2006), "*Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, preventive measures, cash transaction reporting"*, pp. 122-124

[99] World Bank (2006), "*Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, preventive measures, internal controls, compliance and audit"*, page 125

role is taken on by financial intelligence units (FIUs) which use and share financial information with national and international competent authorities to conduct financial investigations. In doing so, each FIU has three main goals[100]:

- *identify, trace, and document the movement of funds;*
- *identify and locate assets that are subject to law enforcement measures;*
- *support the prosecution of criminal activity*.

Generally, within financial intelligence unit, we can distinguish between core functions and additional functions. First of all, it's relevant to state that each FIU is identified as a centralised "recipient" of financial disclosures where financial institutions report and share suspicious information, transactions and other required disclosures; the store of information in a common and centralised repository facilitates both the process of information gathering and analysis.

In executing their functions, financial intelligence units have to first analyse the information (e.g. ordinary deposits, fund transfers) they receive and have access to central databases, advanced techniques and devices and other necessary information in order to detect potential criminal operations linked to money laundering and terrorism financing.

The process of analysing the information is carried on by following a three-step analysis: the tactical one which includes the analysis of basic information and facts behind a criminal offense, the operational one whose aim is to formulate hypothesis on suspicious criminal activities, support investigations through the analysis of the subjects, relationships and targets and finally the strategic analysis which consists in identifying criminal patterns to be used for future analysis by the FIU[101].

After the process of information analysis, a financial intelligence unit has the function to share all the available information to the domestic authorities for further investigation, whether the suspicious operation is driven by money laundering and terrorism financing purposes. In doing so, financial intelligence units closely collaborate with competent domestic authorities as well as with other FIUs worldwide, making information sharing and cooperation between them even more efficient and stronger.

As well as its core functions, each FIU has also some additional functions. One of these is the power of supervision over financial institutions and non-financial business and consequently the power to impose sanction and penalties against them whenever they fail to comply with their obligations, as for instance record-keeping ones. Together with supervisory functions,

[100] World Bank (2006), "*Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, the financial intelligence unit"*, page 128

[101] World Bank (2006), "*Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, the financial intelligence unit, core functions"*, pp. 130-135

FIUs have also regulatory functions since they could be responsible to promulgate regulations to both the financial and reporting sector with reference to the implementation of AML laws[102]. Another important function is strongly related to the analysis core function. Indeed, each FIU can provide support during investigation operations and share information to investigate competent authorities, both necessary to identify suspicious activities. In case of an operation in which a prompt intervention is required, a FIU may be empowered by its country to take temporary measures dealing with it. As a result, it may have the power to block the transaction or preserve the use of an asset.

Last additional functions of a financial intelligence unit concern two important aspect of its action: training and research. In the former case, each FIU has the role to train the personnel working within financial entities, by providing them knowledge, tools and competencies while in the former case each FIU commit to provide research and the results of investigations to its government, after receiving and analysing all the set of financial information.

2.6.5 Data mining techniques

Nowadays, a wide base of transactions is carried out through online operating systems, bank accounts and channels that allow the transfer of funds and personal data exchange. At the same time, these typologies of operations are often viewed as the chance for private subjects and entities to implement hidden and suspicious operations by getting round legal system and competent authorities controls. In this current scenario, possible cases linked to money laundering purposes may take place increasingly making competent authorities and security institutions even more responsible to find more effective solutions to fight against this issue. Indeed, normal auditing procedures and simplified techniques as well as a lack of knowledge and experience in this field represent a real problem for the subjects and institutions involved in the process and in general for a country's economy. This is the reason why more complex and analytical procedures are strictly necessary to detect money laundering and fraud cases. Possible techniques that are currently used through the technology and online data systems and software are related to the method of data mining[103]. Actually, there are several methods that are used for money laundering detection based on different processes and approaches. One of the methods for data mining is based on clustering that consists in gathering most similar subjects data and create a group. In doing so, different groups with very similar information

[102] World Bank (2006), "*Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, the financial intelligence unit, possible additional functions"*, pp. 141-143

[103] Salehi, M., Ghazanfari M., Fathian, M. (2017), "*Data Mining Techniques for Anti Money Laundering, International Journal of Applied Engineering Research"*, pp. 3-6

members are created. This method is usually used to group transactions and match them with bank accounts creating clusters with strong similarities each other. Clustering is also characterised by several insight techniques for the money laundering detection based on different studies and applications. For instance, there is a type of clustering based on the creation of a customer profile where current and history transactions are compared to identify possible reasons for detection. Other possible clustering applications in anti-money laundering are based on a local outlier factor algorithm with the aim to combine clustering techniques and outliers as well as integrating data mining techniques and natural computing by using neural networks and genetic algorithms.

Within data mining, it is possible to identify a three-step approach based on classification, prediction and clustering. In this sense, the classification and prediction approaches are based on a set of logic rules that are used to classify the factors. This is called rule-based methods. One specific technique to make predictions is called "Bayesian network". This technique is based on a model creation to predict future customer transactions according to the past ones. In this case, if a deviation from the original pattern occurs, new transactions will be considered as suspicious for money laundering.

Support vector machine is another technique used to classify and detect activities linked to money laundering. Considering a data set of two classes, the aim of this technique is to find a super-vector which connects the data between two classes, reducing their gap. In this case, statistical learning theory and supper vector machines are used to detect suspicious activities.

Finally, social networks are used for data mining and analysis and to find out distrustful relationship or collaborations between people and entities. Indeed, increasing technology and social network spreading out have fostered virtual exchange of data and their unlawful use for money laundering purposes. In this context, money laundering detection and decision support systems use a wide database to analyse human relationships closely and connect data each other in order to assess the risk of specific profiles and take decisions accordingly.

2.6.6 The FATF and the risk assessment process

In detecting possible cases linked to money laundering purposes, legal entities and financial institutions cooperate with Financial Intelligence Units (FIU) established within the European Union and the Financial Action Task Force (FATF) or GAFI which is an international and independent inter-governmental body whose aim is to devise and promote strategies to combat money laundering, terrorist financing and the financing of proliferation of mass destruction weapons. In doing so, it has laid down an AML framework which includes laws, regulations, enforcements and other measures to allow countries to identify, assess and reduce money

laundering and terrorism financing risks.

Within these functions, each country designates an authority to assess the risks and take proper actions about. Indeed, according to the Recommendation 1 of the FATF[104], "*the goal of the standard is to ensure that countries can mitigate their ML/TF risks effectively and the risk assessment is clearly intended to serve as the basis for application of the risk-based approach*". Policy makers, operational agencies (e.g. law enforcement, FIU), regulators, financial institutions, non-profit organizations adopt a risk-based approach in assessing the nature, scope and operations carried out by a legal entity or organization. In this regard, risk assessment process has to follow some basic principles and phases summarised as follows:

- clear agreement on purpose and scope among all the parties involved in the assessment process. This is generally the willing to help a country to identify, assess and understand ML risks but other goals can be set out;
- determination of the scope, money laundering and terrorism financing;
- level of risk assessment such as national, supranational and sub-national level as well related situations and competent authorities;
- high-level commitment at governmental or European level to recognise and understand any possible ML risks
- planning and organisation of the risk assessment process, which may include working group of experts, round-table discussions, meetings between competent bodies, definition of role, responsibilities and objectives, data gathering and analysis, tools and resources endowment and the frequency of risk assessments.

The risk assessment process can be divided into 3 stages that are the identification, analysis and evaluation. Briefly, in the first stage, causes or drivers of money laundering risks are identified and these referred to specific signals or threats by the involved subjects. Later, the risk analysis and so the nature, sources, probability and possible consequences is carried out with the aim to have a general understanding of each risk. After the risk identification and analysis, the last stage is the evaluation. Since there are several risks with different features, priorities are defined according to the starting purpose and a clear mitigating strategy will be set out.

In this process, the risk identification is definitely the most relevant phase to identify and detect signals of money laundering as a set of threats and vulnerabilities within a country.

Before identifying the risks linked to money laundering, it is necessary to identify those activities or events representing real signals at the base of the offence.

[104] FATF Guidance (2013), "*National Money Laundering and Terrorist Financing Risk Assessment"*, page 5

Here following a list of activities and shortages that represent money laundering warnings[105]:

- the participation in an organised criminal group (e.g. drug, politics) whose proceeds flow into the financial system and mingle with proceeds from legitimate business;
- terrorism or terrorist financing groups that basically raise funds from apparently legal and illegal activities to move these proceeds within the system through cash smuggling, donations or investing in assets (e.g. real estate);
- other illegal activities including trafficking in human beings, sexual exploitation, trafficking in narcotic drugs, illicit arms and stolen goods;
- lack of information about beneficial ownership that fosters criminals to hide their identity and links between them;
- poor monitoring systems not allowing the identification of suspicious transactions by competent financial authorities;
- focus on declared crimes only hinders broader investigations by law enforcement;
- failure to adopt measures to suspend asset transactions during investigations;
- poor money laundering laws making launderers able to avoid the conviction.

These are only a few of the activities that constitute money laundering signals. Criminals are also engaged in a wider base of unlawful activities we have not mentioned before (e.g. corruption, fraud, counterfeiting, extortion).

2.6.7 Money laundering indicators

As well as the above-mentioned activities and shortages in the financial system, there is a series of indicators of unusual transactions of money laundering that auditors, counsellors and other legal consultants may come across to in the exercise of their functions. Specifically, according to the Organization for Economic Cooperation and Development (OECD)[106], there are money laundering indicators for several categories including individuals, business, charities and foreign legal entities, real estate, international trade and others.

With reference to individuals, there is a particular situation called "unusual possession" in which these subjects are not able to justify their expenditures since their income or proceeds come from criminal activities. In this way, they hide the origin of their income by using funds to establish a new business or carry out transactions with third parties. Possessing or using expensive assets with a relative low level of income, obtaining a loan on a low income basis and carrying on unusual transactions such as an asset purchase for a much lower market value

[105] FATF Guidance (2013), "*National Money Laundering and Terrorist Financing Risk Assessment"*, pp. 23-24
[106] OECD (2019), "*Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors"*

or transfer huge amount of cash with a non-comparable level of income represent very suspicious operations and real indicators for money laundering that competent authorities can use to investigate and detect people and organizations in charge. It is clear that this kind of transactions are carried out with undeclared proceeds coming from unlawful operations; these proceeds can also be deposited in a domestic bank account at first and transferred into an offshore bank account afterwards in order to allow further transactions and possible withdrawals[107].

Illicit transfer of funds can lead to the establishment of new business that aim to hide their origin and carry out unlawful operations more and more. Particularly, within a business activity, unusual transactions involving its organization, customers, banks, partners as well as non-identifiable subjects or entities can occur throughout. This is the case for instance of transactions carried on with suspicious customers or without supporting documents and even outside its core business. Moreover, unclear payments and money transfers to and from third parties not engaged in the operations, counterfeit or not-declared bank accounts with a non-defined origin and economic reason as well as transactions accompanied by fictitious deliveries or goods, inflated amounts and unclear documentation represent concrete signals of non-transparent and unusual business operations.

A clear example of illicit transfer of funds comes from the charities and non-profit organizations sectors. Indeed, there may be the risk that transfer of funds has been made unlawfully to support criminal organizations instead of non-profit organizations; in this way, donating individuals or businesses lower their taxable income, being the donation a tax-deductible operation. As we said before, lack of documentation and transparency in transactions involving large amount of cash deposits and transfer of assets are likely giving rise to suspicious operations linked to money laundering and terrorism financing[108].

Another example is given by the real estate sector where several techniques are used to hide and transfer funds illegally. It is the case for instance of a selling operation for a much higher price than the market value or, on the other hand, a purchasing operation in which the criminal is going to pay a part of the amount by cash and the other under the table. Another case occurs when a real estate is rented to a third-party name but actually the real estate is used by the criminal, making both the operation and ownership non-transparent and unlawful.

It is clear that most of the criminal operations are carried out in cash. On one hand, criminals can conceal its origin and give the idea that money derive from a legitimate source apparently

[107] OECD (2019), "*Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors"*, pp. 34-35

[108] OECD (2019), "*Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors"*, pp. 39-40; 43-44

but, on the other hand, cash payments and large amount possession has always been linked to suspicious operations and also has the disadvantage to limit spending and investment possibilities. In this regard, the unusual origin of payments (e.g. countries with corruption or political instability), possession, spending (e.g. luxury goods) and cash flows (e.g. deposits, loans and turnover) represent concrete indicators for criminal operations linked to money laundering[109].

Cash payments and movements of large amount of money take place through international trade as well. In this case, criminals adopt different techniques to conceal criminal proceeds and move the goods across countries. Indeed, goods may be purchased with criminal proceeds in a country and then exported in a new country, also by applying a higher (over-valuation) or lower (under-valuation) price. As we said before, over or under valuations allow to move capital abroad in the form of money flows or goods. Furthermore, when goods are exported or imported, documents such as the invoice and the bill of lading can contain false descriptions or can miss relevant information as regards the price, quantity and quality of goods; it can happen that even when selling or purchasing documents are issued, goods will never be delivered with the aim to move money under the table and hide illegal activities. In addition to the just-mentioned features, these operations are characterised by other suspicious indicators as for instance the risky origin or destination of goods, the creation of new corporations, the transport systems for goods and differences between amount of money paid and invoiced.

One of the most developing payment and investing system in the current scenario is represented by cryptocurrencies, virtual assets based on cryptography language. However, it is also a system through which criminals can disguise the origin of money deriving from unlawful activities by bypassing the presence of a third-party and directly transfer value to another one. Cryptocurrency transactions take place through an online trading platform linked to a digital wallet thanks to the blockchain-based technology that uses new coins to create algorithms and increase the number of transactions. Since this kind of virtual transactions take place anonymously, criminals take advantage of it by making payments using criminal proceeds or converting these currencies into cash. In this case, there are exchange traders and prepaid cryptocurrency cards which allow to obtain and withdraw cash respectively in exchange for cryptocurrencies. Actually, there are several techniques through which tax evaders and criminals in general use cryptocurrency virtual system to carry on unlawful activities and conceal proceeds deriving from them[110]. Among them it is possible to identify large cash

[109] OECD (2019), "*Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors"*, pp. 47-48; 51-52

[110] OECD (2019), "*Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors"*, p. 55-57; 59-61

deposits, large cryptocurrency exchanges and purchases of non-affordable luxury goods with available reported income. Other cases in which involved parties are not able to justify their reason for cryptocurrency operations, disclose each other their identity or the scope of the purchasing is not related to its use represent unusual and risky situations that are likely linked to money laundering and other illicit activities.

2.7 Conclusion

Overall, this chapter focused on the most recent European sources of law with respect to money laundering and described the main techniques implemented by the different subjects involved in the fight against illicit cash activities. Specifically, the most important source of law at European level is the directive 2015/849, in which the European legislator has firstly acknowledged the main criminal activities at the source of money laundering and secondly provided the operative directives for preventing and detecting illegal movements of cash, such as customer due diligence procedures implemented by European countries and competent authorities as well as the obligation for countries and national authorities to make business information and data available to the public through a central registration office. Later, the European Legislator focused its attention on the reporting obligations by FIUs (Financial Intelligence Units) and data collection and protection with the aim to adopt a risk-management approach and prevent money laundering cases. Finally, the Directive provided a description of the policies, procedures and supervision that obliged sectors have to comply with in their country to deal with possible criminal activities linked to money laundering effectively.

Directive 2018/843 is the last up-dated directive on money laundering that introduced some relevant modifications to the directive 2015/849. In particular, main modifications concerned the subjects obliged to comply with AML measures, including also currency exchange providers both legal and virtual, new instruments and dispositions for customer due diligence procedures and to access to confidential ownership information.

Another important European source of law is the Regulation 2015/847. It mainly regulates all those fund transfers in which a payment service provider or intermediary is involved and in particular their obligations about data analysis and protection during the transactions.

Ultimately, we described the main relevant anti-money laundering techniques that competent legal authorities at both European and national level commit to implement in order to identify suspicious activities and prevent the use of financial system for criminal operations.

Third Chapter

The impact of criminal presence on bank lending activity

3.1 Introduction

The previous Chapters explained how money laundering is perpetrated and fought. In Chapter 1 we outlined that banks have always represented a key mechanism for criminals for laundering the proceeds of their illicit activities. In Chapter 2 we saw the important role banks have in preventing and battle money launderers. In Chapter 3 we want to understand the relationship between money laundering organizations and financial institutions at local level, more specifically the potential impact of criminal companies on bank lending activity in Italian municipalities. In other words, the objective of our research is to understand if criminal presence in the Italian territory might discourage financial institutions in lending money to firms and individuals. In the models we are going to develop, we refer to criminal companies as the ones connected to organized crime and used to launder money[111]. This paper in fact follows a series of research in criminal companies conducted by the associate professors of the Dipartimento di Scienze Economiche ed Aziendali "Marco Fanno" of the Università degli Studi di Padova Antonio Parbonetti and Michele Fabrizi. They examined all the verdicts and preventive detection orders issued in Central and Northern Italy from 2004 to 2015 for organized crime conspiracy and mafia-related crime and collected, alongside the Italian Chamber of Commerce (Camera di Commercio) a sample of 1.139[112] companies whose business partners have been convicted for organized crime and money laundering-related crime, according to the Art. 416-*bis* of the Italian Penal Code. The criminal companies of the sample are mostly concentrated on Central and Northern Italy regions, namely Liguria, Lombardia, Piemonte, Valle d'Aosta (north-west), Emilia-Romagna, Friuli-Venezia Giulia, Trentino-Alto Adige, Veneto (north-east), Lazio, Marche, Toscana ed Umbria (center). They were targeted by a police operation during the time span 2004-2015[113] and observed for an average of three and half years each. The decision to focus our analysis on Central and Northern Italy regions depends on the fact

[111] Fabrizi, M., Malaspina, P., Parbonetti, M., "*Caratteristiche e modalità di gestione delle aziende criminali"*, page. 2
[112] http://www.unipd.it/ilbo/mafia-aziende-criminali-nord-italia
[113] Fabrizi, M., Malaspina, P., Parbonetti, M., "*Caratteristiche e modalità di gestione delle aziende criminali"*, page. 1

that criminal companies targeted concentrated mostly in Lombardia (425 companies covering 37,38% of the sample), Veneto (187 companies covering 16,45%) and Liguria (74 companies covering 6,51%). Furthermore, as Mario Draghi outlined during a speech at the Università degli Studi di Milano on March 11th 2011[114], organized crime is deeply-rooted in South Italy to politically control the territory, while deeply-infiltrated in the North to perpetrate illicit financial crimes, such as money laundering and usury.

The analysis we are going to develop in this Chapter is carried out throughout Stata program.

3.2 Criminal presence in Central and Northern Italy

Before approaching the description, investigation and interpretation of data throughout Stata, we are going to illustrate criminal presence in Italy, by detailing why criminals invest their proceeds in companies located in different Italian territories, such as Northern and Central regions as compared to Southern ones. As reported in the research[115] "Progetto PON Sicurezza 2007-2013: Gli investimenti delle mafie" by Transcrime about the investments of mafia organizations, criminal groups are differently present in the Italian territory. By using the IPM (index of mafia presence, that combines the measurement of murders and attempted murders, people reported to authorities for mafia association, municipalities dissolved for mafia-related crimes, goods seized to organized crime and active organizations on the Italian territory), the research showed that criminal groups, although being present in all regions, are more pervasive in Southern regions, where they originated. As shown in table 1 below, Campania, Calabria, Sicilia and Puglia have the higher value of IPM, while Veneto, Trentino Alto Adige and Molise have the lower.

Criminal organizations in the former regions are present in small groups of variable size that produce a high concentration, especially in Campania, where "Camorra" is well known for being composed by many different families controlling different portions of the territory. Conversely, criminal organizations in the latter are scattered and produce a lower concentration. Criminals invest their profit from illicit activities for a variety of purposes: first, to conceal it from the authorities, throughout money laundering or transportation of illegal goods. Second, to exploit the profitability of an economic sector by controlling companies and by infiltrating in the economic fabric or third, to maximize their social consent by creating jobs for the population.

[114] *Le Mafie a Milano e nel Nord: aspetti sociali ed economici,* Intervento del Governatore della Banca d'Italia, Mario Draghi, Milano, 11 marzo 2011

[115] Transcrime. 2013. "*Progetto PON Sicurezza 2007-2013: Gli investimenti delle mafie. Rapporto Linea 1.*" Milano: Ministero dell'Interno. www.investimentioc.it

Table 1. Index of mafia presence (IPM) at regional level

Rank	Region	IPM
1	Campania	61,21
2	Calabria	41,76
3	Sicilia	31,8
4	Puglia	17,84
5	Lazio	16,83
6	Liguria	10,44
7	Piemonte	6,11
8	Basilicata	5,32
9	Lombardia	4,17
10	Toscana	2,16
11	Umbria	1,68
12	Emilia Romagna	1,44
13	Abruzzo	0,74
14	Sardegna	0,7
15	Marche	0,67
16	Valle d'Aosta	0,57
17	Friuli Venezia	0,42
18	Veneto	0,41
19	Trentino Alto	0,37
20	Molise	0,31

Source: Transcrime 2013, Progetto PON, page 27

Furthermore, criminal organizations are driven by strategic aims, namely controlling the territory and by cultural ones, such as imposing their manner of conducting business. In this context, while criminal presence in Northern and Central regions is branched to primarily exploit the wealth of the territory throughout illicit economic activities, in the South is concentrated to politically control the territory. In fact, the influence of Mafia in Northern and Central regions is hidden[116], while in Southern regions Mafia is pervasive and exercise a strict control the territory. We decided to focus the analysis on Central and Northern regions to understand criminal activity through financial crime and to describe the way organized crime exploits companies to invest its proceeds in the legal economy and clean them. Northern regions represent for criminal organizations the most desirable area of the country for the economic opportunities they offer. In these regions, criminal organizations invest their illicit proceeds to acquire stake in companies in order to camouflage launder their illicit proceeds into the legal

[116] Reganati F., Oliva, M., (2017), "*The Determinant of Money Laundering: Evidence from Italian Regions"*, Department Digef, Sapienza, Rome, Italy, Economics and Financial Market freelance journalist, Rome, Italy, page 8

economy. According to Venturini and Brachi (2017), Lombardia, Veneto and Emilia Romagna have been chosen colonized by criminal organizations both for necessity and for opportunity[117]: in the first case, they have been colonized by the criminals that have been compulsorily confined by the Italian Institutions (necessity); in the second, they possessed the perfect characteristics for Mafia to carry on illicit activities such as drug trafficking and extortion and to reinvest the proceeds of those activities into the legal economy through money laundering (opportunity).

3.3 The dataset

After having explained the background of the research, we are going to describe the dataset we will analyze and the variables that will be involved in our models.

As previously mentioned in the introduction of Chapter 3, the analysis we are going to develop follows a series of research in criminal companies conducted within the Dipartimento di Scienze Economiche ed Aziendali "Marco Fanno" of the Università degli Studi di Padova. The primary database (hereafter "Criminal Companies Database") was merged with the secondary database (hereafter "Enviromental Variables Database") in order to build up the explanatory models. The Criminal Companies Database is a panel dataset of companies observed in multiple years with one of the following characteristics:

- They have been seized by Italian authorities for mafia-related crimes;
- Their business partners have been convicted for organized crime and money laundering-related crime;
- A person convicted for mafia-related crimes had a business stake in the companies of at least 10%.

The identification of the companies was possible since from 1982 the Italian Penal Code have been specifically regulating mafia-related crimes through article 416-bis, which defines mafia groups in the following way:

"*si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri, ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali*"[118]. As such, mafia groups are the ones

[117] Venturini, G., Branchi, M. (2017), "*Il rapporto tra mafia e impresa: il caso della 'Ndrangheta nell'economia lombarda*", page 27

[118] https://www.brocardi.it/codice-penale/libro-secondo/titolo-v/art416bis.html

that exploit the strength of the organizations to commit crimes, to obtain directly or indirectly the control of economic activities or to make unfair profits.

The companies have been observed in a time span of 10 years, from 2005 to 2014. No observations prior to 2005 have been considered in our analysis since information were not available and we wanted to ensure comparability of data. For each company, the dataset contains corporate data such as the Tax Code, the Business Name, the Municipality where the company had its administrative offices, the Province and the "ATECO " code, which is a manner of classification used by Italian national institute of Statistics ISTAT ("Isitituto Nazionale di Statistica Italiano") and expresses the business where the company operates. Furthermore, the dataset contains the financial statement figures according to the Italian Civil Code for each company observed, such as for instance the value of assets and liabilities, receivables and payables, cash in bank and debt to financial institutions, that will be used to build up some of the explanatory variables of the model.

The Enviromental Variables Database is a panel database of municipalities observed from 2005 to 2015 that contains the following data:

- Loans, deposits and branches by municipality, respectively the amount in Euro of loans granted by financial institutions to the private sector, the amount in Euro of bank deposits from the private sector and the number of bank counters at municipality level. The data have been collected from the "Infostat section" of the Banca d'Italia website[119], inquiring for the report "TDB10194". "*The data refer to all the Italian municipalities in which the number of banks is sufficient to ensure the confidentiality of the data and the number of branches in each municipality in which there is at least one bank is also shown. The data on deposits refer only to registered accounts. In December 2010, some changes in the stocks of loans and deposits were the result of a redistribution of customers within the branch network following a major banking consolidation"*[120]*;*
- Average income at municipality level, that measures the amount in Euro of average income declared yearly by individuals for tax purposes (IRPEF) at municipality level. The data have been collected from the website of the Italian Ministry of Economic Development ("Ministero dello Sviluppo Economico")[121], inquiring for the report "Dichiarazioni Fiscali" within the statistical analysis section[122];

[119] https://infostat.bancaditalia.it

[120]https://infostat.bancaditalia.it/inquiry/#eNorSazIt3IOdXINdg2xDQh1cvKJNzCogTHiDQzjDYx0PENcfYNdfVyjbENcnAwNDC1NdPwDXP1s%0A0xJzilP1yzJTy8FGeLoEwxXoFxdUpuckFhfrAwCZfR1L

[121] http://www.finanze.gov.it/

[122] http://www1.finanze.gov.it/finanze3/pagina_dichiarazioni/dichiarazioni.php

- Number of inhabitants at municipality level, extrapolated from ISTAT website[123]
- Percentage of inhabitants with high school and college education at municipality level. The indicators were calculated by dividing the number of inhabitants of the municipality with respectively college education and high school education by the number of total inhabitants of the municipality. The percentage has been calculated for the year 2011 (when the last Italian census took place) and was applied to all the years of observation;
- Average percentage of inhabitants that participated to the referendums that took place in Italy from 1993 to 2016 at provincial level. The data were extrapolated from the website of the Ministry of Internal Affairs of the Italian Government[124];
- Average percentage of inhabitants that participated to the referendum that took place in Italy from 2011 to 2016 at municipality level. The data were extrapolated from the website of the Ministry of Internal Affairs of the Italian Government and 2011 is the first year when the data are available at municipality level.

We adopted data at municipality level to catch the highest possible level of detail, in order to reduce measurement errors and to ensure variability of the data. Italy is fragmented in more than eight thousand municipalities with deep differences in social, economic and financial development amongst them. Just think Italy alone constitutes the most varied linguistic heritage of all Europe with more than thirty dialects currently spoken other than Italian language itself within the Italian territory and according to Istat Italy alone had more than 4,3 million active companies in 2015. As such, data at municipality level best control for cross-sectional differences among provinces and regions. During the period 2005-2015 the Italian municipalities have undergone a process of unification for spending review purposes disciplined by the D.Lgs. n.267/2000[125]. As a consequence, the number of municipalities passed from over 8101 in 2001[126] to 8.048 in 2015[127]. Both databases were adapted in order to transpose the effect of the unification and not to lose variability of the dataset.

In order to lay the foundation of some descriptive statistics the dataset was elaborated and cleansed. At first, we created three variables that, sorting for the municipality and the year of observation, expressed the number of criminal companies at municipality level, the value of total assets of the criminal companies and municipality level and the average of Ebitda divided by the value of assets respectively. At second, we merged the Criminal Companies Database and the Enviromental Variables Database. Finally, we dropped from the newly created database

[123] http://dati.istat.it/Index.aspx?DataSetCode=INDUNIV#
[124] https://elezionistorico.interno.gov.it
[125] D.Lgs. n.267/2000
[126] http://www.comuniverso.it/index.cfm?Comuni_dal_1861&menu=12
[127] http://www.comuniverso.it/index.cfm?Comuni_dal_1861&menu=12

all the observations for which the number of branches by municipality was less than three and the value of loans and deposits was equal to zero in order to ensure the comparability of data.

3.4 The research variables

The aim of this paragraph is to describe the variables involved in the model in order to lay down the main hypothesis on how these variables might work together. The dependent variable is the number of "Criminal companies" observed each year from 2005 to 2014 at municipality level, labelled as "TOT_CRIM". Usually crime variables are negatively influenced by underreporting, since, within the total population of offences occurred in a time span, some might not be reported by the victims to the authorities. In our analysis this potential issue is addressed and solved by the fact that data of criminal companies are obtained from investigations made by police authorities and, as such, not dependent from reporting. The independent variables are explained in the following sub-paragraphs.

3.4.1 Bank and firm controls

The aim of both bank and firm control variables is to grasp differences in the ability of the borrowers to solve their liabilities and in their demand for credit[128]:

- "LOANS", namely the amount in Euro of loans granted by financial institutions to the private sector, which represents a proxy of the investment of the banking sector into the real economy and ultimately a measure of the trustworthiness of the private sector;
- "DEPOSITS", namely the amount in Euro of bank deposits by the private sector, which represents a proxy of the wealth of the municipality and ultimately a measure of its financial development;
- "BRAN_INHAB", namely the number of bank branches within the municipality, which, together with the variable "DEPOSITS", represents a proxy of the financial development of the municipality;
- "TOT_ASSETS", namely the ratio between the amount in Euro of total assets of the criminal companies and total assets of the municipality where they are located, which measures the development of the firm within its area of operations. Bigger firms in term of size are usually more likely to be granted a loan, since they have more assets to be offered as collateral.
- "MEAN_PERF", namely the ratio between EBITDA (Earnings before taxes,

[128] Bonaccorsi di Patti, E. (2009), "*Weak institutions and credit availability: the impact of crime on bank loans"*, Banca d'Italia Questioni di Economia e Finanza, page 11.

depreciation and amortization) and total assets of the criminal companies expressing the ability of the criminal company to generate cash and ultimately to be profitable from an operating perspective.

3.4.2 Enviromental variables

Enviromental variables are included in the model to control for the characteristics of both economic and socio-cultural background in which the companies operate.

- "PC_INCOME", namely income per capita, which is the ratio between the total income of the municipality and the number of its inhabitants. This is a proxy of the wealth and economic development of the municipality;
- "UNI_EDUC", namely university education, which is the ratio between inhabitants with college education and total inhabitants of the municipality measured in 2011, the year in which the last Italian census took place. This is a proxy of cultural development of the municipality;
- "MUN_PART", namely municipality electoral participation, which is the ratio between eligible inhabitants that participated to the referendum that took place in Italy from 1993 to 2016 at provincial level and total eligible inhabitants. This variable represents a proxy of the social capital and social development of the province and ultimately of the municipalities in the province.

3.5 The research hypothesis

As mentioned in the previous paragraphs, the aim of this research is to study the relationship between criminal presence at municipality level and bank lending activity, controlling both for bank and firm characteristics and socio-economic and cultural characteristics of the municipality in which the firms operate. Before approaching the analysis throughout Stata, we want to outline the expected relationship among variables and the hypothesis we want to verify throughout the empirical analysis.

In the following tables we are outlining the expected relationships among dependent and independent variables, based on the information available in the economic literature so far. In table 2 below we present the expected relationship among firm and bank controls. As outlined by Emilia Bonaccorsi di Patti, the presence of criminal firms "*indirectly affects investment by reducing the availability of credit and distorting loan terms and conditions*"[129], in other words

[129] Bonaccorsi di Patti, E. (2009), "*Weak institutions and credit availability: the impact of crime on bank loans"*, Banca d'Italia Questioni di Economia e Finanza, page 20.

should negatively affect the propensity of financial institutions to grant loans. Thus, we can formulate the first hypothesis we want to test throughout our model.

HP1: Criminal presence at municipality level reduces the amount of credit granted by financial institutions to the private sector.

Nevertheless, we expect the presence of criminal firms to be positively linked to the economic and financial development of the territory, since criminal organizations are more eager to seep in wealthy territories to drain their financial resources, rather than in poor and isolated ones.

HP2: "The number of criminal companies is higher in municipalities where the economic and financial development is higher."

Furthermore, the relationship between criminal firms and their size and operating performance depends on the intrinsic characteristics of the companies. Usually small companies in term of assets are used to support the criminal organizations and their performance is weak since they apparently not carry out any productive activity[130], while medium firms are used to launder money and their performance is volatile. Finally, firms with good performance are used to seep in the political and social context.
The propension of financial institutions to grant loans depends on multiple factors, namely the past experience with the customers, their creditworthiness, the presence of collaterals and so on. Usually, the higher the economic and financial development of the territory, the higher the amount of loans banks can grant. For what concerns the relationship among amount of loans, dimension and performance of the criminal companies, we have to consider different factors. Since the main focus of criminal companies considered in our analysis is money laundering, we would expect companies financing themselves through the proceeds of illegal activities rather than demanding for loans to financial institutions. However, the capability of criminal organizations to put under pressure the management of the political, administrative and banking system, might in some cases grant higher access to credit. As such, the relationship between amount of loans and dimension of the companies might depend on the characteristics of the companies themselves. According to Transcrime, we can divide criminal companies in three categories[131]: "productive", "screen" and "paper". "Productive" companies perform economic

[130] Fabrizi, M., Malaspina, P., Parbonetti, M., "*Caratteristiche e modalità di gestione delle aziende criminali"*, page. 3
[131] Transcrime. 2013. "*Progetto PON Sicurezza 2007-2013: Gli investimenti delle mafie. Rapporto Linea 1.*" Milano: Ministero dell'Interno. www.investimentioc.it, page 191

activities and as such might require higher financial resources to be invested in long-term assets used in production and, consequently, higher amounts of loans. “Screen” companies are only used for money laundering and do not perform any economic activities. Consequently, they might not require loans by financial institutions. “Paper” companies, although having the same characteristic of “screen” companies, are used by criminal organizations to invest the proceeds of illicit activities in formally legal investments in fixed and non-fixes assets, cars and other financial activities, in order to disguise the effective property of these assets and protect them from seizure. “Paper” companies might require access to credit by financial institutions. The link between the amount of loans granted by financial institutions to the private sector and the economic performance of criminal companies depends on the characteristics of the companies. “Productive” companies are usually profitable and, as such, might require higher amount of loans to finance their activities and exploit tax deductions of financial expenses, while “screen” and “paper” companies are usually not profitable and as such might not exploit the aforementioned tax deductions.

As previously explained, the amount of deposits and branches as proxies for economic development should be positively correlated with the amount of loans and branches, since, the higher the deposits by the private sector in the banking system, the higher amount of resources the banking system can grant to the private sector and the higher the number of branches to be opened to serve the territory. The relationship between economic development and dimension and profitability of criminal companies depends on the characteristics of the criminal companies.

Table 2. Expected relationship among firm and bank controls

Firm and bank controls	**TOT_CRIM**	**LOANS**	**DEPOSITS**	**BRAN_INHAB**	**TOT_ASSETS**	**MEAN_PERF**
TOT_CRIM	n/a	-	+	+	+	-
LOANS	-	n/a	+	+	+	+
DEPOSITS	+	+	n/a	+	+	+
BRAN_INHAB	+	+	+	n/a	+	+
TOT_ASSETS	+/-	+	+	+	n/a	+
MEAN_PERF	+/-	+	+	+	+/-	n/a
PC_INCOME	+	+	+	+	+	+
UNI_EDUC	-	+	+	+	+	+
MUN_PART	-	+	+	+	+	+

Source: Personal elaboration

In table 3 below we outline the expected relationship among environmental variables.
We expect per capita income to be positively related with the presence of criminal companies in the territory since criminal companies, especially in Northern regions, usually seep in the economic fabric to drain financial resources.

HP3: "The number of criminal companies is higher in municipalities where income per capita is higher".

Per capita income should also be positively related with the amount of loans, deposits and branches of the municipality, since the higher the income of a territory, the higher the deposits and the propension of financial institution to develop their business. At this preliminary stage the relationship between per capita income and both size and performance of the criminal companies is uncertain: we could expect the relationship to be positive, since the higher the wealth of a territory, the higher the possibility for criminal companies to do business, to increase their assets and improve their performance . Nevertheless, the penetration of criminal companies in a specific territory might discourage old and new investors to develop their business thus reducing the overall income. For what concerns the relationship between per capita income and education, the economic literature provides plenty of studies. We mention here Barro and Lee telling that economic growth is positively related with the level of education, since educated workers are more eager to understand and apply new technologies[132] and the higher the technological development, the higher the potential for economic growth[133]. According to the economic literature, economic development is positively related to social capital. First of all, for social capital we mean the definition by Fukuyama, namely "*an instantiated informal norm that promotes cooperation between two or more individuals*"[134]. Second, we have evidence from Helliwell and Putnam that income levels in Italy are higher in regions with more social capital[135], since the combination of civic sense, institutional performance and citizen satisfaction in some regions compared to others drove in the 80s greater levels of economic growth.
As we have just described the possible relationship between education and economic development, we are now going through the relationship between education, criminal presence

[132] Barro, R. J., Jong-Wha Lee (2002), "*Education and Economic Growth*", page 31
[133] Robert, M. Solow (2010), "*Stories about economics and technology*", The European Journal of the History of Economic Thought, pp. 1113-1126
[134] Fukuyama, F. (2000), "*Social capital and civil Society",* International Monetary Fund working paper, page 3
[135] Helliwell, J. F., Putnam, R. D. (1995), "*Economic growth and social capital in Italy",* Eastern Economic Journal, Vol. 21, No.3, Summer 1995

and both size and performance of criminal companies. The economic literature provided many proofs regarding the relationship between education and crime since the early 50s. For instance, unequal distribution of schooling is strongly related to the incidence of many crimes according to Ehrlich[136] and the probability of committing crimes decreases with years of education according to Groot[137]. As such, we expect the relationship between education and crime to be negative.

HP4: "Criminal presence at municipality level is lower in municipalities where education is on average higher."

Furthermore, when it comes to the relationship between education and size and performance of criminal companies, results are not unambiguous. Assuming education to be negatively correlated with crime, we would expect highly educated municipalities having small-size and non-profitable criminal presence. Nevertheless, criminal companies continuously adapt their manning to new regulations and new repression methods by authorities, finding new ways to commit illicit activities. As such, we might expect both criminal organizations to attract highly-educated with the promise of a greater and faster remuneration and criminals to be financially and economically educated. We will investigate further in our empirical analysis the possible implications of the relationship between education and characteristics of the criminal companies. Finally, we would expect the relationship between education and electoral participation to be positively correlated, since both of them can be included in the definition of social capital.

The last set of expectations we want to express regards electoral participation at municipality level as a proxy for social development. According to Buonanno (2009), "civic and altruistic norms and associational networks significantly reduce crime rates" and "a policy of promotion of civic norms and associational life may have beneficial side effects in terms of crime-reduction."[138]. As such, we expect criminal presence to be lower in municipalities where social development is higher.

HP5: "The higher the social development at municipality level, the lower the criminal presence."

[136] Ehrlich, Isaac (1975), "*On the Relation between Education and Crime*", Education, Income, And Human Behavior F. Thomas Juster, ed, page 335.
[137] Groot, W. (2010), "*The effects of education on crime*", Article on applied Economics, page 20.
[138] Buonanno PAGE, Montolio D., Vanin PAGE (2009), "*Does social capital reduce crime?",* Quaderni di ricerca del Dipartimento di Scienze Economiche "Hyman PAGE Minsky", The Journal of Law and Economics pp. 11-12.

After having spoken of the relationship with criminal presence, we want to focus on economic and financial development. Also, in this case we have plenty of studies in the economic literature so far. Among the most significant for the purpose of our analysis, we can point out Guiso, Sapienza and Zingales (2001). Following the work of Putnam[139], they detailed the connection between social capital and a relevant factor of economic growth, namely financial development. More in depth, social capital for the aforementioned authors refers to the "*aggregate of the actual or potential resources which are linked to possession of a durable network of more or less institutionalized relationships of mutual acquaintance and recognition, or in other words, to membership in a group, which provides each of its members with the backing of the collectively-owned capital, a "credential" which entitles them to credit, in the various senses of the word*"[140]. Higher investments in stocks instead of cash, higher access to credit from financial institutions and less use of informal credit[141] are present in areas of Italy with high levels of social capital. As such, we would expect social development to be positively linked to financial development. Ultimately, it is difficult to make assumptions regarding the relationship between social development and size and performance of criminal companies.

Table 3. Expected relationship among environmental variables

Enviromental variables	PC_INCOME	UNI_EDUC	MUN_PART
TOT_CRIM	+	-	-
LOANS	+	+	+
DEPOSITS	+	+	+
BRAN_INHAB	+	+	+
TOT_ASSETS	+	+	+
MEAN_PERF	+	+	+
PC_INCOME	n/a	+	+
UNI_EDUC	+	n/a	+
MUN_PART	+	+	n/a

Source: Personal elaboration

3.6 The empirical analysis

Now that we have described the dataset, the embedded variables and formulated our hypothesis,

[139] Putnam, R. (1995), "*The Case of Missing Social Capital*", Harvard University working paper.
[140] Bourdieu PAGE (1985), "*The forms of capital.*" In Handbook of Theory and Research for the Sociology of Education, ed. JG Richardson, pp. 241-58.
[141] Guiso, L., PAGE Sapienza, and L. Zingales (2004), "*The role of social capital in financial development*", American Economic Review, 94, pp. 526–556.

we are going to analyze the population of the dataset through some basic descriptive statistics and carry out the empirical analysis.

3.6.1 The population

The number of observations represents the number of times the phenomenon is observed. In this case we are observing a municipality during a time span of ten years, from 2005 to 2014. In table 4 below we represent the number of observations per region, in other words how many times the municipalities of the below mentioned regions are observed:

Table 4. Observations per region

Region	**Observations**	**Percentage**
Lombardia	5.069	27%
Veneto	3.353	18%
Emilia Romagna	2.363	12%
Piemonte	1.896	10%
Toscana	1.806	10%
Lazio	1.105	6%
Friuli Venezia Giulia	923	5%
Marche	825	4%
Trentino Alto Adige	619	3%
Liguria	471	2%
Umbria	386	2%
Valle D'Aosta	94	0%
Total	18.910	100%

Source: Personal elaboration

As we can see almost 78% of our observations is concentrated in northern regions (Lombardia, Veneto, Emilia Romagna, Piemonte, Friuli Venezia Giulia, Trentino Alto Adige, Liguria and Valle D'Aosta) while the remaining 22% in central ones. Furthermore, as we can see in table 5 and 6 of Appendix 1, the number of observations per region is stable for all the regions involved in our analysis. This means we are observing a stable number of municipalities in our time span. As outlined in table 5 of Appendix 1, the criminal presence is observed within our dataset 806 times (4,3% of the observations). 670 criminal companies (83%) out of 806 are concentrated, as mentioned in paragraph 3.1, in northern regions, such as Lombardia (282), Veneto (168), Piemonte (94), Emilia Romagna (70), Liguria (28), Friuli Venezia Giulia (20) and Trentino Alto Adige (8), while 136 (the remaining 17%) in central ones. In the following table 7 we present some descriptive statistics of the variables we will include in our models.

Table 7. Summary statistics of the variables

Variables	Mean	Standard Deviation	Minimum	Maximum	Median	25% Percentiles	75% Percentiles
TOT_CRIM	0,12	1,54	0	58	0	0	55
LOANS	402.104	4.169.766	353,00	181.845.244	93.540	53.825	187.062
DEPOSITS	762.631	9.571.004	215,00	423.815.902	133.811	69.552	297.088
BRANCHES	12,58	51,98	3,00	1.615,00	5,00	4,00	9,00
TOT_ASSETS	1.721,06	51.615	0	3.293.397	0	0	2.355.335
MEAN_PERF	(0,00)	0,11	(7,85)	5,23	0,00	(2,94)	0,97
PC_INCOME	12.709	2.091,75	5.047,52	28.965	12.637	11.378	13.938
UNI_EDUC	0,08	0,03	0	0,25	0,07	0,58	0,91
MUN_PART	0,55	0,04	0,36	0,68	0,55	0,52	0,58

Source: Personal elaboration of Stata output

The mean of the variables varies from -0,0002 for percentage of performance of criminal companies to Euro 762.631 for amount of deposits at municipality level. Furthermore, standard deviation, which measures the dispersion of the dataset with respect to its mean, varies from 0,03 for percentage of college education to Euro 4.169.766 for loans at municipality level. Consequently, we can understand there's heterogeneity in the values of the variables. Minimum varies from 0 for the number of criminal companies at municipality level to -7,85 for the percentage of performance of companies. Note also that the minimum number of branches is three: this is because the Bank of Italy does not spread data of deposits and loans for municipalities with less than three branches for privacy purposes. Maximum varies from 0,25 for the percentage of inhabitants at municipality level with college education to Euro 423.815.902 for deposits at municipality level. Median, which is the value separating the higher hand from the lower hand of a distribution, varies from 0 for the number of criminal companies to 133.811 for the amount of deposits at municipality level. The 25% percentile varies from 0 for the number of criminal companies to 69.522 fro the amount of deposits, while the 75% percentile varies from 0,91 for the percentage of inhabitants with college education to 2.355.335 for the amount of total assets of criminal companies. In appendix 1 we can find the histograms of the aforementioned variables compared with the normal distribution.

After having outlined the main descriptive statistics, we are now dividing the population in two different sub-groups with respect to the aforementioned variables in order to run the *t-test*. The purpose of the *t-test* is to verify if the means of two subgroups are equal: if the null hypothesis is true, it means that any difference between the two means is due to chance and the statistical analysis cannot produce a satisfactory output. We divide the population in the following sub-groups: municipalities with criminal presence and municipalities without criminal presence.

We summarize the output of the *t-test* in the following tables.

Table 8.1. T-test with respect to loans

Criminal companies	Obs	Mean	Std. Error
0	18.104	242.033,9	12.999,6
1	806	3.997.528,0	636.064,9
Sum	18.910		
t	=	-25,4427	
Pr(|T| > |t|	=	0,0000	

Source: Personal elaboration of Stata output

The observation column shows that we have 18.910 observations, of which 18.104 are non-criminal companies and 806 are criminal companies. The Mean coloumn highlights that criminal companies have higher amount of loans compared to non-criminal companies. Furthermore, the table shows that the group means are significantly different since the p-value in the Pr|T| > |t| row is 0,0000: as a consequence, we can reject the null hypothesis with a 5% significance level.

Table 8.2. T-test with respect to deposits

Criminal companies	Obs	Mean	Std. Error
0	18.104	421.767,5	24.523,8
1	806	8.418.938,0	1.513.206,0
Sum	18.910		
t	=	-23,5479	
Pr(|T| > |t|	=	0,0000	

Source: Personal elaboration of Stata output

The Mean coloumn highlights that criminal companies have higher amount of deposits compared to non-criminal companies. Furthermore, the table shows that the group means are significantly different since the p-value in the Pr|T| > |t| row is 0,0000: as a consequence, we can reject the null hypothesis with a 5% significance level.

Table 8.3. T-test with respect to branches

Criminal companies	Obs	Mean	Std. Error
0	18.104	9,9	0,2
1	806	73,6	7,7
Sum	18.910		
t	=	-35,1519	
Pr(|T| > |t|	=	0,0000	

Source: Personal elaboration of Stata output

The Mean coloumn highlights that criminal companies have higher amount of branches per inhabitant compared to non-criminal companies. Furthermore, the table shows that the group means are significantly different since the p-value in the Pr|T| > |t| row is 0,0000: as a consequence, we can reject the null hypothesis with a 5% significance level.

Table 8.4. T-test with respect to per capita income

Criminal companies	Obs	Mean	Std. Error
0	18.104	12.668,5	15,4
1	806	13.623,6	78,8
Sum	18.910		
t	=	-12,7372	
Pr(|T| > |t|	=	0,0000	

Source: Personal elaboration of Stata output

The Mean coloumn highlights that criminal companies have higher amount of per capita income compared to non-criminal companies. Furthermore, the table shows that the group means are significantly different since the p-value in the Pr|T| > |t| row is 0,0000: as a consequence, we can reject the null hypothesis with a 5% significance level.

Table 8.5. T-test with respect to university education

Criminal companies	Obs	Mean	Std. Error
0	18.104	0,7662	0,0002
1	806	0,0937	0,0013
Sum	18.910		
t	=	-17,1061	
Pr(|T| > |t|	=	0,0000	

Source: Personal elaboration of Stata output

The Mean coloumn highlights that criminal companies have lower amount of university education compared to non-criminal companies. Furthermore, the table shows that the group means are significantly different since the p-value in the Pr|T| > |t| row is 0,0000: as a consequence, we can reject the null hypothesis with a 5% significance level.

Table 8.6. T-test with respect to municipality participation

Criminal companies	Obs	Mean	Std. Error
0	18.104	0,5502	0,0003
1	806	0,5545	0,0013
Sum	18.910		
t	=	-2,9326	
Pr(|T| > |t|	=	0,0034	

Source: Personal elaboration of Stata output

The Mean coloumn highlights that criminal companies have lower amount of municipality participation compared to non-criminal companies. Furthermore, the table shows that the group means are significantly different since the p-value in the Pr|T| > |t| row is 0,0000: as a consequence, we can reject the null hypothesis with a 5% significance level.
All in all, we can conclude that the null hypothesis is rejected in all models and we can proceed with further analysis of the database.

3.6.2 Correlation matrix

In table 9 of Appendix 2 we are presenting the correlation matrix among the variables we are going to include in our model, in order to verify if, at a first glance, we can identify patterns among variables consistent with our expectations and hypothesis. The correlation matrix provides a first explanation of the relationship among variables, telling the change in value of one variable if another variable changes. The correlation coefficient expressed in our matrix represents a quantitative assessment that gages both the way and power of the propensity of the variables to fluctuate together.
First of all, we can notice that the correlation between municipality participation and the other explanatory variables is not statistically significant, except for per capita income college education and branches per inhabitant. Consequently, no interpretation for municipality participation is provided at this stage of the research, but further analysis will be performed in the following paragraphs.
Consistently with our expectations, criminal presence at municipality level is positively correlated with deposits and per capita income, but the correlation with branches per inhabitant is not statistically significant. Economically and financially developed municipalities attract on average more criminal companies; parallelly, criminal companies establish their business in rich areas where they can both perform illicit activities such as drug trafficking and prostitution and reinvest their illicit proceeds into companies for the purpose of money laundering. Incoherently with our hypothesis, criminal presence is positively correlated with loans and

college education. At this first stage of our research we can say that on average criminal companies are more present in areas where the availability of loans is higher. The correlation between criminal presence and size is positive, since, the higher the former, the higher the investments made by criminal organizations in the territory. The correlation with performance is negative and significant at 5% level: we can outline that on average criminal companies are not driven by making profit, but by exploiting the richness of the territory throughout illicit activities.

The availability of loans is positively correlated with deposits, per capita income and college education at municipality level. Consistently with our expectations, the higher the wealth and education of the municipality, the higher the availability of credit by financial institutions. The correlation with size of criminal companies is positive, while the one with performance is negative. On average, criminal companies invest more where the availability of credit is higher, but their performance stays poor, since they are not interested in making profit, but in exploiting the wealth of the area.

The amount of deposits at municipality level positively correlates with per capita income and college education: the higher the richness and education of private people, the higher the presence of financial institutions in the territory. As for loans, the amount of deposits is positively correlated with total assets of criminal companies and negatively correlated with their performance, probably for the aforementioned explanations.

The presence of branches per inhabitant is positively correlated with per capita income and education. The higher the richness of the private sector, the higher the presence of financial institutions in the area. With respect to size and performance of criminal companies, the correlation is not statistically significant.

While the correlation between total assets of criminal companies and their performance is not significant, the correlation with per capita income and education is positive and significant.

Ultimately, per capita income is positively correlated with education, consistently with our expectations.

3.6.3 Univariate and multivariate linear regression

After having outlined the correlation among the variables, we are now analyzing the relationship between our independent variables, namely “LOANS” and “TOT_CRIM”, which express respectively the amount in Euro of loans by financial institutions and the number of criminal companies observed at municipality level during the time span 2005-2014, and the independent variables, in order to test for the hypothesis we have outlined in paragraph 3.4.

3.6.3.1 Univariate linear regression

First of all, we are going to check the *univariate linear regression* with the objective to understand the 1:1 relationship between criminal presence and explanatory variables.

As outlined by table 10 below, although the relationship with municipality participation is not statistically significant, the relationship among all others explanatory variables is positive and statistically significant at 1% level of confidence. What can we gather from the above table? Is the univariate regression providing empirical evidence supporting our hypothesis or not? HP1 is not supported by empirical evidence in model (1), since it appears that criminal presence increases if the availability of loans increases, although the coefficient is very little: it means that for every new criminal company at municipality level, loans increase on average by Euro 1,8 million. HP2 is supported by empirical evidence only with respect to deposits in model (2), meaning that for every increase by one Euro of deposits, criminal presence increases by 0,000000106 and 0,0233. HP3 tested in model (4) is supported by empirical evidence too, meaning that for every increase by one Euro of per capita income criminal presence increases by 0,0000730. Ultimately, we cannot gather any information supporting HP5 tested in model (6) since the relationship is not statistically significant.

Table 10. Univariate linear regression

	(1) LOANS	(2) TOT_CRIM	(3) TOT_CRIM	(4) TOT_CRIM	(5) TOT_CRIM	(6) TOT_CRIM
TOT_CRIM	1870378.3335***					
	(13.64)					
DEPOSITS		0.0000***				
		(5.53)				
BRAN_INHAB			-60.7935***			
			(-3.62)			
PC_INCOME				0.0001***		
				(5.47)		
UNI_EDUC					7.6927***	
					(6.06)	
MUN_PART						0.0689
						(0.44)
_cons	181832.7224***	0.0367***	0.1625***	-0.8104***	-0.4773***	0.0798
	(10.14)	(3.62)	(8.63)	(-5.06)	(-5.44)	(0.89)
N	18910	18910	18907	18910	18910	18910
adj. R-sq	0.477	0.436	0.000	0.010	0.020	-0.000

t statistics in parentheses
* p<0.05, ** p<0.01, *** p<0.001

Source: Stata output

3.6.3.2 Multivariate linear regression

After having analyzed the results of *univariate linear regression*, we are now outlining the Stata

output for *multivariate linear regression* or *multiple linear regression* model. The *multivariate linear regression* is similar to *univariate linear regression*, except for the fact that the model has multiple independent variables to explain the dependent variable. The standard model is exemplified by the following formula[142]:

$$Y_i = B_0 + \beta_1 X_{1 + \ldots +} \beta_p X_p + \varepsilon_i$$

where:

Y_i is the dependent variable;

X_i (X_1, X_2, …, X_p) is the independent variable;

$\beta_0 \in R$ is the intercept;

β_1 $\beta_p \in R$ is the regression coefficients;

ε_i is the error term.

We are going to develop multiple models through including different explanatory variables.

Model 1: Loans as a function of Criminal Presence and Bank Controls

$$LOANS\_M_i = B_0 + B_1(TOT\_CRIM) + B_2(DEPOSITS\_M) + B_3(BRAN\_INHAB) + \varepsilon_i$$

Model 2: Loans as a function of Criminal Presence and Environmental Controls

$$LOANS\_M_i = B_0 + B_1(TOT\_CRIM) + B_2(UNI\_EDUC) + B_3(MUN\_PART) + B_4(PC\_INCOME\_M) + \varepsilon_i$$

Model 3: Loans as a function of Criminal Presence, Bank Controls and Environmental Controls

$$LOANS\_M_i = B_0 + B_1(TOT\_CRIM) + B_2(DEPOSITS\_M) + B_3(BRAN\_INHAB) + B_4(UNI\_EDUC) + B_5(MUN\_PART) + B_6(PC\_INCOME\_M) + \varepsilon_i$$

Model 4: Loans as a function of Criminal Presence, Bank Controls, Environmental Controls and Firm Controls

$$LOANS\_M_i = B_0 + B_1(TOT\_CRIM) + B_2(DEPOSITS\_M) + B_3(BRAN\_INHAB) + B_4(UNI\_EDUC) + B_5(MUN\_PART) + B_6(PC\_INCOME\_M) + B_7(MEAN\_PERF) + B_8(UNI\_EDUC) + \varepsilon_i$$

Model 5: Criminal presence and Bank Controls

$$TOT\_CRIM_i = B_0 + B_1(LOANS\_M) + B_2(DEPOSITS\_M) + B_3(BRAN\_INHAB) + \varepsilon_i$$

[142]https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3049417/

Model 6: Criminal Presence and Enviromental Controls

$$TOT\_CRIM_i = B_0 + B_1(UNI\_EDUC) + B_2(MUN\_PART) + B_3(PC\_INCOME\_M) + \varepsilon_i$$

Model 7: Criminal Presence, Bank Controls and Firm Controls

$$TOT\_CRIM_i = B_0 + B_1(LOANS\_M) + B_2(DEPOSITS\_M) + B_3(BRAN\_INHAB) + B_4(TOT\_ASSETS) + B_5(MEAN\_PERF) + \varepsilon_i$$

Model 8: Criminal Presence, Bank Controls and Enviromental Controls

$$TOT\_CRIM_i = B_0 + B_1(LOANS\_M) + B_2(DEPOSITS\_M) + B_3(BRAN\_INHAB) + B_4(UNI\_EDUC) + B_5(MUN\_PART) + B_6(PC\_INCOME\_M) + \varepsilon_i$$

Model 9: Criminal Presence, Firm Controls and Enviromental Controls

$$TOT\_CRIM_i = B_0 + B_1(TOT\_ASSETS) + B_2(MEAN\_PERF) + B_3(UNI\_EDUC) + B_4(MUN\_PART) + B_5(PC\_INCOME\_M) + \varepsilon_i$$

Model 10: Criminal Presence, Bank Controls, Firm Controls and Enviromental Controls

$$TOT\_CRIM_i = B_0 + B_1(LOANS\_M) + B_2(DEPOSITS\_M) + B_3(BRAN\_INHAB) + B_4(UNI\_EDUC) + B_5(MUN\_PART) + B_6(PC\_INCOME\_M) + B_7(TOT\_ASSETS) + B_8(MEAN\_PERF) + \varepsilon_i$$

Where:

LOANS_M = LOANS/1000

DEPOSITS_M = DEPOSITS/1000

PC_INCOME_M = PC_INCOME/1000

HP1 is tested through the models in table 10 of Appendix 2: the coefficient is statistically significant in all models, however it is positive in models (1) and (2) and negative in models (3) and (4). Consequently, we cannot gather any particular conclusion regarding HP1 at this stage of the research.

HP2, HP3, HP4, HP5 are tested in table 11 of Appendix 2. The coefficient for the variable "LOANS_M" is negative and statistically significant in models (3) and (6), therefore criminal presence is negatively correlated with the amount of loans. Furthermore, in models (3) and (6) the coefficients for the variable "DEPOSITS_M" are positive and statistically significant, therefore we have empirical evidence that in municipalities with criminal presence the amount of deposits is on average higher. In every model the variable "BRANCHES" is negatively correlated with the number of criminal companies, as such HP2 is not supported by empirical

evidence at this stage of the research. The coefficients for the variable "UNI_EDUC" are significant at 5% level for all models except for model (5), as such HP4 is not supported by evidence at this stage of the research. Probably the most significant result of is the one in model (6), which has an R^2 of 0,708 as compared to the other models, telling that on average the higher the education, the lower the criminal presence. However, at this stage we have to be careful in the interpretation of the results, since linear regression models are subject to *multicollinearity* among variables and a high R^2 might be the red flag. Consequently, we are going to adopt panel data regression models to control for *multicollinearity*. The coefficients for the variable "MUN_PART" are negative and significant at 5% confidence level except for model (6). This means that on average higher social development drives lower criminal presence. The coefficients for the variable "PC_INCOME_M" are always positive and significant at 5% confidence level, meaning that criminal companies are on average more present if the private sector is richer, except for model (5) in which the coefficient is not statistically significant.

3.6.4 Panel data regression

The linear regression models we have just analyzed provide some preliminary insights on the research, but the results cannot be considered sufficient since the models do not capture the panel dimension of our database. As explained in the introduction to chapter 3, our database is built on two dimensions, namely the municipalities where the companies are observed and the years in which they are observed together with the other explanatory variables. We are now going to run regressions with panel data in order to control for the year and the municipality of observation, thus including more variability in the data and reducing *collinearity* among variables. *Collinearity* arises when there's high correlation among two or more explanatory variables. While *cross-sectional analysis* takes a picture of the data in a certain moment in time, *panel analysis* allows to study the variation in time of data, thus providing better estimated parameters. The general model of *panel data* at time t is the following:

$$Y_{it} = B_0 + \beta_1 X_1 t_1 + \ldots + \beta_p X_p t_p + u_{it}$$

Where

Y_{it} is the dependent variable at time t;

$X_i t_i$ ($X_1 t_1$, $X_2 t_2$, …, $X_p t_p$) is the independent variable at time t;

$\beta_0 \in R$ is the intercept;

β_1 β_p $t_p \in R$ is the regression coefficients at time t;

u_{it} is the residual standard deviation at time t;

and $i = 1 \rightarrow N$ and $t = 1 \rightarrow T$.

The residual term u_{it}, which indicates all the non-observed variables, can be divided in two

parts: α_i and ε_{it}. α_i is the term that indicates the constant of every statistical unit *I*, and takes into consideration the effect of a set of variables not observed constant in time on the depedent variable. α_i is usually called *unobserved factors* or *fixed effect* or *non-observed heterogeneity* and is time invariant, in other words it is not direct function of time. The error term ε_{it} is called *time-varying error*, because it represents the random error term that influences the depedent variable Y_{it}. This term is similar to the error term in a simple linear regression model, For the econometrical analysis of *panel data,* we cannot assume that the observations are independently distributed in time, in other words that each random variable has the same probability distribution as the others and all of them are mutually independent (iid). Consequently, in order to control for these characteristics, we are going to adopt the so-called *fixed-effects model.*

In a *fixed-effects model* the term u_{it} is represented by the following equation:

$uit = \alpha i + \varepsilon it$, where

- αi is the part of the error dependent from the observed unit and independent from time, which includes the effect of all the non-observable variables and;
- εit is the part of the error of the single observation.

The *fixed-effects model* focuses on the elimination of the part of the error αi, in order to exclude non-observable values as part of the error in the model. These values might be correlated with the explanatory variables, thus providing a distorted estimation.

3.6.4.1 Univariate Panel data regression

In table 12 below we are outlining the results of univariate panel data regression controlling for *fixed-effects*.

Table 12. Univariate panel linear regression

	(1) LOANS_M	(2) TOT_CRIM	(3) TOT_CRIM	(4) TOT_CRIM	(5) TOT_CRIM	(6) TOT_CRIM
TOT_CRIM	-581.0*					
	(-2.23)					
DEPOSITS_M		-0.0000123				
		(-0.15)				
BRAN_INHAB			542.3**			
			(2.84)			
PC_INCOME_M				-33.14***		
				(-3.85)		
UNI_EDUC					-7.683***	
					(-4.40)	
MUN_PART						0
						(.)
_cons	470.5***	0.127*	-0.281*	0.539***	0.712***	0.118***
	(15.34)	(1.99)	(-2.00)	(4.93)	(5.27)	(2.17e+10)
N	18910	18910	18907	18910	18910	18910
adj. R-sq	0.285	0.000	0.002	0.001	0.006	.

t statistics in parentheses
* p<0.05, ** p<0.01, *** p<0.001

Source: Stata output

In model (1) the relationship between the criminal presence at municipality level and loans is negative. This represents the very first empirical evidence supporting HP1, telling that, on average, the increase of criminal companies by one unit is associated with a decrease of the amount of loans by financial institutions by Euro 581 thousand. The relationships between criminal presence and the variables "DEPOSITS_M" and MUN_PART", controlling respectively in models (2) and (6) for the economic development and social development of the municipalities, are not statistically significant. Consequently, HP5 cannot be supported by empirical evidence at this stage of the research. The relationship between criminal presence and the variable "BRAN_INHAB", which controls for the economic and financial development of the municipality level in model (3), is positive and statistically significant: on average, if an increase in branches by one unit, is associated with an increase in the presence of criminal companies by 542 units. This is the very first result supporting HP2. HP3, tested in model (3), is not supported by empirical evidence, since the relationship between criminal presence and per capita income is negative and statistically significant. Finally, the relationship between criminal presence and the percentage of people with college education at municipality level tested in model (5) is negative and statistically significant, thus providing empirical evidence in support of HP4. The coefficient of determination, the so called R^2, which gives insight regarding the specification of a statistical model, is close to zero for models 4 and 5. This means the models are not correctly specified and probably more explanatory variables should be included in the model for better estimation purposes. Consequently, we proceed with *multivariate panel data regression* in the following paragraph.

3.6.4.2 Multivariate Panel data regression

After having analyzed the results of *univariate panel data regression,* we are now outlining the Stata output for *multivariate panel data regression*. The objective of the analysis is, as previously explained, to test the hypothesis described in paragraph 3.5. The models we are going to exploit are the same as in paragraph 3.6.3.2, except for the fact that the regressions are built on panel data. The panel dimension is captured observing the data taking into consideration both the municipality and the year in which it is observed. This means we are trying to understand the relationship among variables considering different municipalities observed during a time span of ten years, from 2005 to 2015. First of all, we want to investigate the relationship between criminal presence and the amount of loans by financial institutions at municipality level. The models we are looking at in order to test HP1 are the ones in table 13

of Appendix 2. Except for model (3), the coefficient for TOT_CRIM, which measures the number of criminal companies at municipality level, is always negative and statistically significant. Controlling only for bank variables in model (1), we can highlight that municipalities with higher number of the criminal presence area associated with a lower the amount of loans by financial institutions. In particular, increasing the criminal companies by one unit, on average the amount of loans is associated with a decrease in the amount of loans by approximately half a million Euro (-567.3). This result is consistent with the result of the *univariate panel regression* in paragraph 3.6.4.1. Furthermore, we can notice the positive relationship between loans and deposits, as expected. Controlling only for environmental variables in model (2), the coefficient is negative and statistically significant at 5% confidence level, while the environmental variables are not statistically significant. Controlling for bank, environmental and firm variables in model (4), the coefficient "TOT_CRIM" is equal to -741.6 and statistically significant. Furthermore, the coefficient for deposits and total assets of criminal companies are positive and statistically significant. The models, which are robust for *heteroskedasticity* and control for *fixed-effects*, confirm the hypothesized negative relationship between criminal companies and the amount of loans granted by financial institutions at municipality level.

In table 14 of Appendix 2 we are testing the hypothesis from 2 to 5. First of all, we can see that the negative relationship between criminal presence and the amount of loans is confirmed in every model. Second, the relationship between criminal presence and deposits and branches is always positive and statistically significant. As such, HP2 is supported by empirical evidence in our models: on average, criminal presence is associated with financially developed municipalities. Third, the relationship between criminal presence and per capita income is not homogeneous in all models: in models (2) and (4), which respectively control for environmental variables only and for both environmental and firm variables, the coefficients are positive and statistically significant at 1% confidence level, while in model (5) which controls for environmental and bank variables the relationship is negative and statistically significant at 5% level of confidence. Fourth, the relationship between criminal presence and education is negative in all models except for model (5), but significant only in models (2) and (4). As such we have empirical evidence supporting HP4: on average, criminal presence is lower where the level of education is higher in our models. Fifth and last, the relationship between criminal presence and municipality participation is not statically significant, thus HP5 is not supported by empirical evidence.

3.7 Conclusion

The Chapter focused on the analysis of the relationship between criminal companies and the specific context in which they develop their business taking into consideration multiple characteristics such as its economic, financial, social and cultural development. Our investigation in fact follows a series of other research conducted within the Università degli Studi di Padova with the aim to understand the role of companies in the process of money laundering. To conduct our analysis, we employed a database of criminal companies at municipality level mainly located in Northern and Central Italy targeted by a police operation for money laundering and mafia-related offences from 2004 to 2005. We focused our inquiry especially in the municipalities of Northern and Central Italy, where criminal organizations establish their business to primarily exploit the greater economic and financial development as compared to Southern ones. After having explained our database through descriptive statistics, we outlined the expected relationship among the variables included in the database and ultimately formulated our five hypothesis. We tested them through both linear and panel regression models, controlling for the year and the municipality of observation. Both linear and panel regressions confirmed the negative relationship we expected between loans and criminal presence outlined in HP1 and the positive relationship expected between loans, deposits and branches outlined in HP2. HP3 tested as expected under linear regression models, while results were not consistent with our expectations under panel regression models. The negative relationship expected between criminal presence and level of education outlined in HP4 was confirmed under panel regression models only. Finally, the hypothesis of negative relationship between criminal presence and social development under HP5 was confirmed under linear regression models, but not statistically significant under panel regression models.

Conclusion

Over the past decade, despite the regulatory measures to tackle money laundering at Italian, European and global level are continuously growing and becoming more and more accurate, the phenomenon has increased both in strength and pervasiveness in the financial system. Criminal organizations are always looking for new methods to clean the proceeds of their illicit activities, and to make them disposable again, in order to be invested and reintroduced into the legal economic system. Indeed, all the efforts put in place by the authorities seem not to be sufficient to reduce the economic and social costs of the problem. The only way to tackle the phenomenon is to deepen the knowledge of it, through a punctual analysis of the academic studies and literatures, combined with the observation of actual money laundering cases registered at local level. The more information we retrieve, the more we will be prepared to recognize and contrast the phenomenon in the near future. The objective of the academic research carried out in the latest decade, as well as the objective of this particular study, goes exactly in this direction, aiming at providing the authorities, the regulators and the main subjects involved in the process, with insights on the development of money laundering phenomenon among companies at local level, highlighting its economic and social costs within the Italian territory. Therefore, this research was carried out with the final purpose to measure the impact of money laundering into the economic context, particularly focusing on its influence on bank lending activity.

In Chapter 1 we reviewed the existing literature, determining that the phenomenon takes place usually through a three-stage process of placement, layering and integration of funds, and permeates the economic fabric at all levels, but especially banks and other financial institutions: these represent the principal vehicles used by launderers to turn their criminal proceeds into disposable amounts for future investments.

In Chapter 2 we analysed the currently existing regulation at European level and acknowledged that the legislator, through the emanation of the Directives 2015/849, 2018/843 and the Regulation 2015/847, provided the financial system with instruments to fight the spread of money laundering. Some of the most relevant measures implemented are customer due diligence procedures, reporting obligations by FIUs (Financial Intelligence Units) at single state level, as well as data collection and protection.

Moreover, as a result of the literature review carried out in Chapter 1 and 2, we understood the key role of banks in the fight against money laundering.

Therefore, in Chapter 3 we conducted an accurate analysis to understand how the operating

business of banks, with a particular focus on the activity of lending, is influenced by the presence of companies involved in money laundering processes, dedicating special attention to their outcomes in the Italian local municipalities.

Our statistical analysis, both with linear and panel data regressions, confirmed the evidence provided by the economic and academic literature: indeed, money laundering is detrimental to the economic, social and cultural development of the Italian municipalities. More specifically, we observed that the increase in number of criminal companies involved in money laundering results in a reduction of the amount of loans granted by banks to the private sector, especially in the geography of the Central and Northern Italian municipalities observed in the investigation. Moreover, we assessed that criminal organizations establish their business and criminal companies in municipalities of Central and Northern Italy where the economic development and wealth are greater, in order to drain resources from the legal economy, with the objective to foster the development of the illegal one.

Furthermore, coherently with the economic literature observed, we also registered that a higher level of education reduces the presence of criminal companies in the municipalities, thus providing clear proofs that investing in the education of the society at local level can reduce and discourage the presence of illicit activities in that economic framework.

As a conclusion, through this research, we also achieved to give evidence of the important role that the education of people plays in fighting money laundering, in order to avoid the economic costs that the diffusion of the phenomenon has on the financial development of the Italian municipalities.

Appendix 1

Table 5. Observations per region

REGION	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	Total
Lombardia	415	424	423	443	447	494	496	492	482	476	477	5.069
Veneto	298	299	303	308	312	312	313	310	304	299	295	3.353
Emilia Romagna	209	212	213	215	216	219	219	217	216	214	213	2.363
Piemonte	171	171	170	171	173	173	174	174	174	172	173	1.896
Toscana	158	162	165	167	164	166	167	166	166	163	162	1.806
Lazio	96	97	96	99	100	102	106	106	103	101	99	1.105
Friuli Venezia Giulia	85	85	85	85	86	85	85	83	82	81	81	923
Marche	69	70	71	71	72	81	79	80	78	77	77	825
Trentino Alto Adige	55	56	57	57	57	57	57	57	56	56	54	619
Liguria	45	45	43	43	43	43	43	43	42	41	40	471
Umbria	34	34	36	36	36	37	37	35	34	34	33	386
Valle D'Aosta	8	9	9	8	8	8	9	9	8	9	9	94
Total	1.643	1.664	1.671	1.703	1.714	1.777	1.785	1.772	1.745	1.723	1.713	18.910

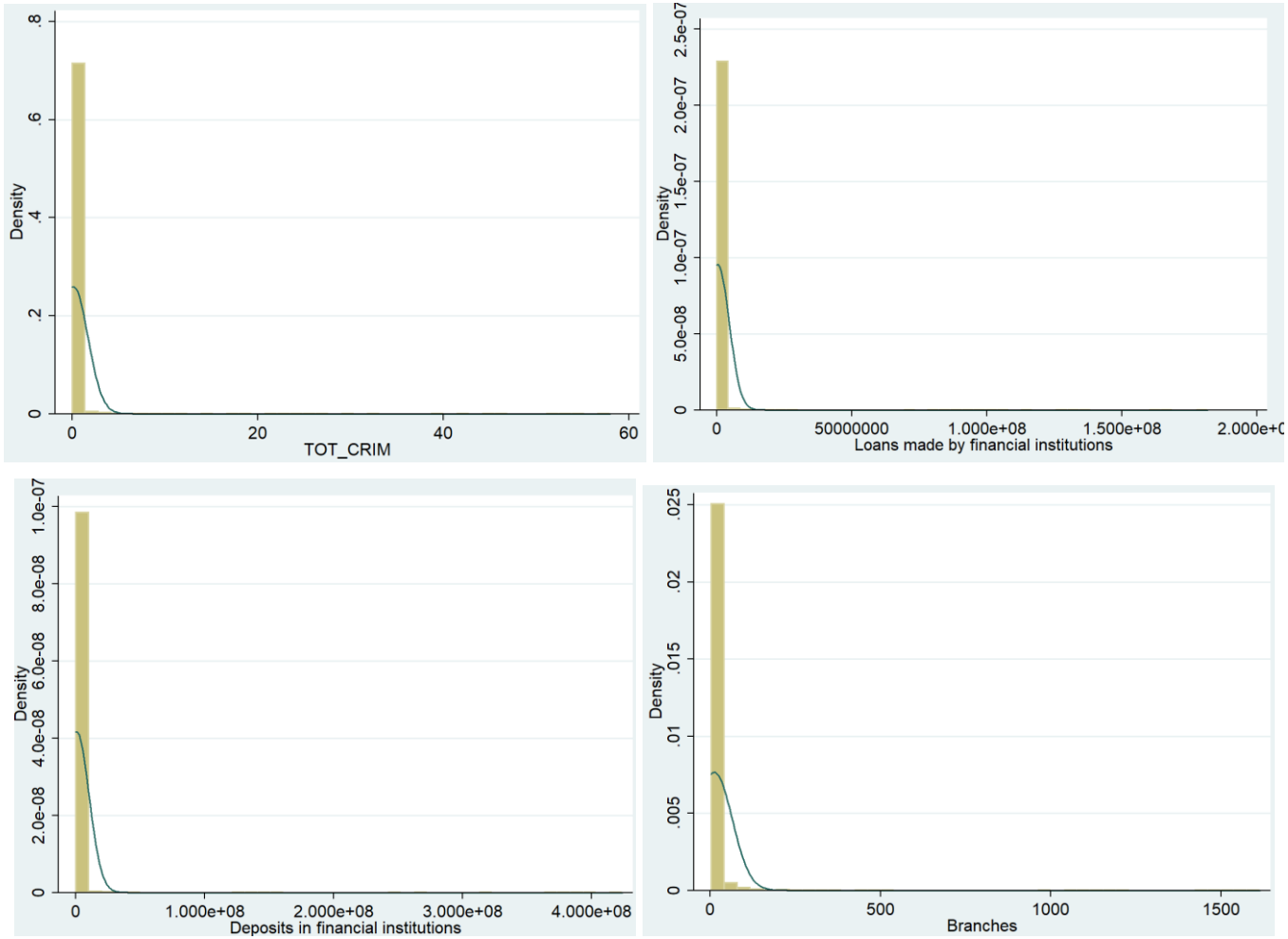
Source: Personal elaboration

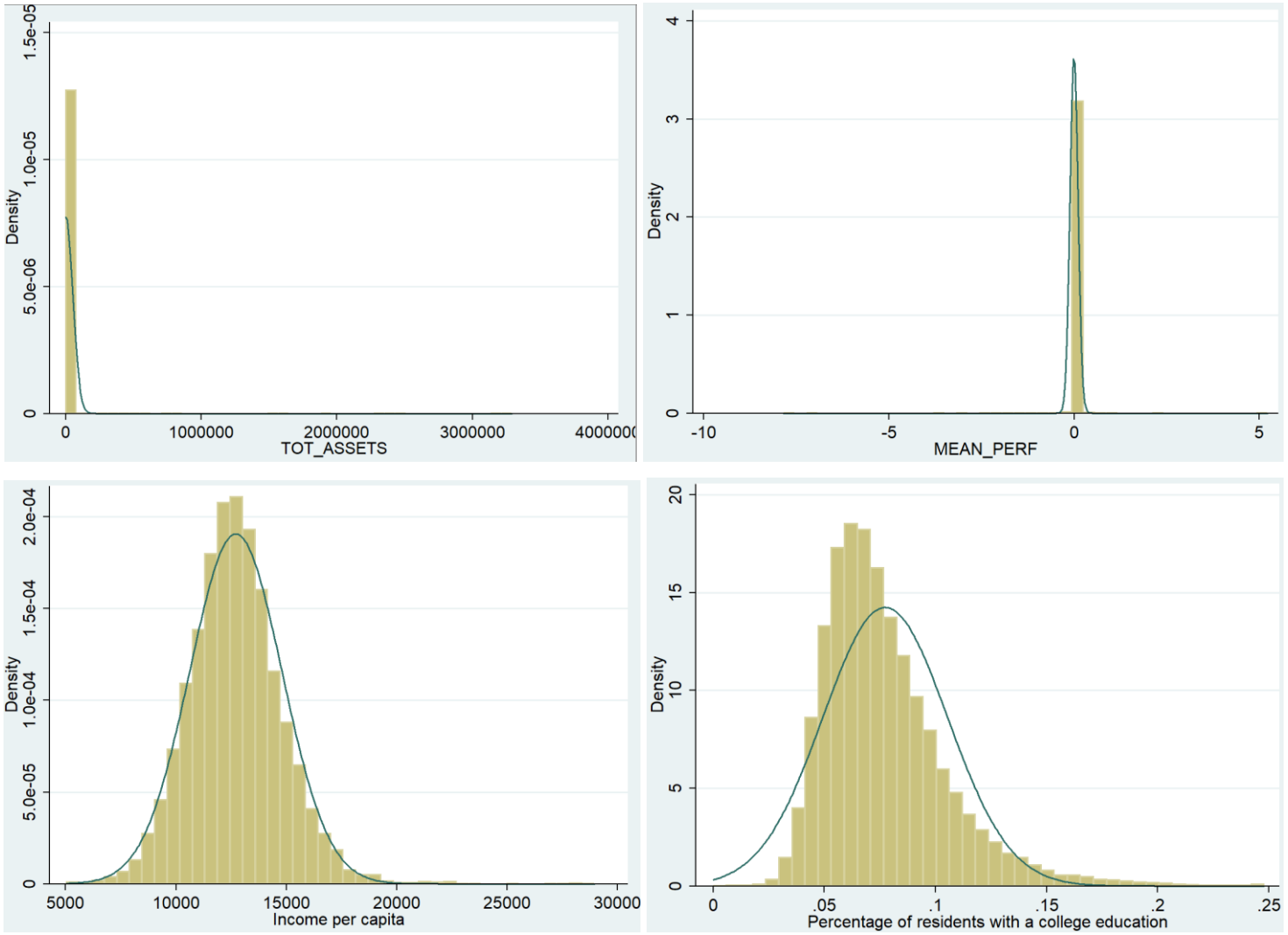
Table 6. Criminal companies per region

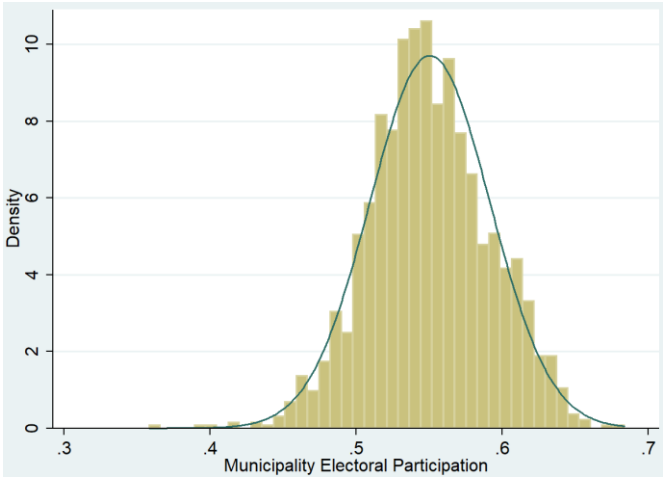
Criminal companeis	Emilia Romagna	Friuli Venezia Giulia	Lazio	Liguria	Lombardia	Marche	Piemonte	Toscana	Trentino Alto Adige	Umbria	Veneto	Total
1	46	19	62	8	203	1	66	34	8	4	112	563
2	14	1	3	11	39	-	12	11	-	-	30	121
3	9	-	-	8	23	-	7	4	-	-	14	65
4	1	-	-	-	2	-	-	4	-	-	4	11
5	-	-	-	1	2	-	-	1	-	-	-	4
6	-	-	-	-	2	-	-	1	-	-	-	3
7	-	-	-	-	1	-	-	1	-	-	-	2
8	-	-	-	-	-	-	-	1	-	-	-	1
9	-	-	-	-	1	-	-	-	-	-	-	1
10	-	-	-	-	-	-	1	-	-	-	-	1
12	-	-	-	-	1	-	-	-	-	-	1	2
15	-	-	-	-	-	-	1	-	-	-	-	1
17	-	-	-	-	1	-	-	-	-	-	1	2
18	-	-	-	-	-	-	1	-	-	-	-	1
21	-	-	-	-	-	-	1	-	-	-	-	1
22	-	-	-	-	-	-	1	-	-	-	1	2
23	-	-	-	-	-	-	1	-	-	-	1	2
24	-	-	-	-	-	-	1	-	-	-	-	1
25	-	-	-	-	-	-	1	-	-	-	1	2
26	-	-	-	-	1	-	1	-	-	-	-	2
27	-	-	-	-	-	-	-	-	-	-	2	2
29	-	-	-	-	1	-	-	-	-	-	1	2
30	-	-	-	-	1	-	-	-	-	-	-	1
32	-	-	1	-	-	-	-	-	-	-	-	1
40	-	-	-	-	1	-	-	-	-	-	-	1
42	-	-	1	-	-	-	-	-	-	-	-	1
45	-	-	2	-	-	-	-	-	-	-	-	2
46	-	-	1	-	-	-	-	-	-	-	-	1
52	-	-	-	-	1	-	-	-	-	-	-	1
53	-	-	1	-	-	-	-	-	-	-	-	1
54	-	-	1	-	-	-	-	-	-	-	-	1
55	-	-	1	-	1	-	-	-	-	-	-	2
57	-	-	1	-	-	-	-	-	-	-	-	1
58	-	-	-	-	1	-	-	-	-	-	-	1
Total	70	20	74	28	282	1	94	57	8	4	168	806

Source: Personal elaboration

Table 7. Distribution of the variables




Density
0
5.0e-06
1.0e-05
1.5e-05
0
1000000
2000000
3000000
4000000
TOT_ASSETS
Density
0
1
2
3
4
-10
-5
0
5
MEAN_PERF
Density
0
5.0e-05
1.0e-04
1.5e-04
2.0e-04
5000
10000
15000
20000
25000
30000
Income per capita
Density
0
5
10
15
20
0
.05
.1
.15
.2
.25
Percentage of residents with a college education



Source: Stata Output

Appendix 2

Table 9. Correlation matrix – Stata output

Variables	TOT_CRIM	LOANS	DEPOSITS	BRAN_INHAB	TOT_AS~S	MEAN_P~F	PC_INC~E	UNI_EDUC	MUN_PART
TOT_CRIM	1								
LOANS	0,6908***	1							
	0,0000								
DEPOSITS	0,6606***	0,9514***	1						
	0,0000	0,0000							
BRAN_INHAB	-0.0130	0.0004	0.0118	1					
	0.0741	0.9537	0.1058						
TOT_ASSETS	0,7297***	0,5775***	0,4196***	-0.0109	1				
	0,0000	0,0000	0,0000	0.1333					
MEAN_PERF	-0,0175*	-0,0262***	-0,0305***	-0.0080	0,0021	1			
	0,016	0,0003	0,0000	0.2736	0,7761				
PC_INCOME	0,0992***	0,1544***	0,1462***	0.0458***	0,0520***	-0,0058	1		
	0,0000	0,0000	0,0000	0.0000	0,0000	0,4278			
UNI_EDUC	0,1399***	0,2159***	0,1941***	-0.0282***	0,0898***	-0,0068	0,6084***	1	
	0,0000	0,0000	0,0000	0.0001	0,0000	0,3479	0,0000		
MUN_PART	0,0018	-0,0097	-0,0109	-0.2195***	0,0037	0,0077	0,2001***	0,1307***	1
	0,8002	0,1804	0,1343	0.0000	0,6069	0,2925	0,0000	0,0000	

p-values in parentheses
* p<0.05, ** p<0.01, *** p<0.001

Table 10. Multiple linear regression - loans

	(1) LOANS_M	(2) LOANS_M	(3) LOANS_M	(4) LOANS_M
TOT_CRIM	298.2*	1821.8***	-5.51e-13**	-309.4***
	(2.02)	(13.57)	(-2.70)	(-38.97)
DEPOSITS_M	0.383***		-4.67e-16***	0.394***
	(14.28)		(-3.50)	(404.76)
BRAN_INHAB	-107517.3***		1.54e-10***	-120472.7***
	(-4.93)		(5.49)	(-5.60)
UNI_EDUC		16224.8***	9.51e-13	4558.6***
		(7.46)	(1.11)	(14.60)
MUN_PART		-3116.6***	7.92e-13**	-740.7***
		(-4.07)	(3.10)	(-4.22)
PC_INCOME_M		54825.7*	-6.52e-11***	4832.2
		(2.35)	(-10.66)	(1.15)
LOANS_M			1.000***	
			(3.17e+15)	
TOT_ASSETS				0.0225***
				(114.95)
MEAN_PERF				-39.28
				(-0.62)
_cons	154.2***	-48.93	1.71e-13	181.9
	(6.80)	(-0.52)	(1.71)	(1.79)
N	18907	18910	18907	18907
adj. R-sq	0.912	0.493	1.000	0.949

t statistics in parentheses
* p<0.05, ** p<0.01, *** p<0.001

Source: Stata Output

Table 11. Multiple linear regression – other variables

	(1) TOT_CRIM	(2) TOT_CRIM	(3) TOT_CRIM	(4) TOT_CRIM	(5) TOT_CRIM	(6) TOT_CRIM
LOANS_M	0.000242		-0.000235*		0.000243	-0.000240**
	(1.86)		(-2.57)		(1.85)	(-2.60)
DEPOSITS_M	0.00000609		0.000157***		0.00000592	0.000158***
	(0.11)		(4.31)		(0.11)	(4.32)
BRAN_INHAB	-64.17***		-78.51***		-56.36***	-82.22***
	(-5.18)		(-8.76)		(-3.81)	(-7.86)
UNI_EDUC		6.961***		3.278***	-0.462	1.243*
		(5.96)		(6.11)	(-0.54)	(2.28)
MUN_PART		-0.747**		-0.529*	0.294*	-0.176
		(-2.67)		(-2.31)	(2.44)	(-1.84)
PC_INCOME_M		19.26*		20.67**	-2.745	5.769*
		(2.18)		(2.73)	(-0.76)	(2.33)
TOT_ASSETS			0.0000205***	0.0000216***		0.0000206***
			(6.52)	(6.81)		(6.53)
MEAN_PERF			-0.0840	-0.259		-0.0832
			(-0.78)	(-1.42)		(-0.78)
_cons	0.0631**	-0.254***	0.115***	-0.144***	-0.0343	0.0460
	(3.09)	(-4.91)	(8.92)	(-3.58)	(-0.54)	(0.95)
N	18907	18910	18907	18910	18907	18907
adj. R-sq	0.477	0.020	0.708	0.539	0.477	0.708

t statistics in parentheses
* p<0.05, ** p<0.01, *** p<0.001

Source: Stata Output

Table 13. Multivariate panel regression – loans

	(1) LOANS_M	(2) LOANS_M	(3) LOANS_M	(4) LOANS_M
TOT_CRIM	-567.2**	-579.3*	1.97e-13	-741.6***
	(-3.20)	(-2.21)	(0.01)	(-4.53)
DEPOSITS_M	0.367***		-8.12e-17	0.336***
	(22.61)		(-0.00)	(17.31)
BRAN_INHAB	-115914.2**		-2.34e-11	-65981.4
	(-3.09)		(-0.00)	(-1.38)
UNI_EDUC		746.6	-2.94e-12	-171.1
		(0.30)	(-0.00)	(-0.12)
MUN_PART		0	0	0
		(.)	(.)	(.)
PC_INCOME_M		46680.0	1.61e-11	16433.7
		(1.33)	(0.00)	(1.29)
LOANS_M			1***	
			(4.58e+13)	
TOT_ASSETS				0.0105***
				(4.67)
MEAN_PERF				-145.4
				(-1.34)
_cons	274.0***	-180.7	-1.14e-13	68.25
	(9.97)	(-0.64)	(-0.00)	(0.77)
N	18907	18910	18907	18907
adj. R-sq	0.624	0.287	1.000	0.721

t statistics in parentheses
* p<0.05, ** p<0.01, *** p<0.001

Source: Stata Output

Table 14. Multivariate panel regression – other variables

	(1) TOT_CRIM	(2) TOT_CRIM	(3) TOT_CRIM	(4) TOT_CRIM	(5) TOT_CRIM	(6) TOT_CRIM
LOANS_M	-0.000739***		-0.000767***		-0.000736***	-0.000765***
	(-13.30)		(-25.67)		(-13.04)	(-25.66)
DEPOSITS_M	0.000264***		0.000237***		0.000263***	0.000237***
	(11.09)		(9.84)		(11.14)	(9.81)
BRAN_INHAB	230.1*		157.6*		95.54	63.19
	(2.53)		(2.47)		(1.49)	(1.19)
UNI_EDUC		-12.39***		-10.83***	-6.334**	-4.473***
		(-3.71)		(-3.94)	(-3.09)	(-3.61)
MUN_PART		0		0	0	0
		(.)		(.)	(.)	(.)
PC_INCOME_M		80.83**		64.59**	54.39*	39.67**
		(2.71)		(3.21)	(2.43)	(2.95)
TOT_ASSETS			0.0000134***	0.0000122***		0.0000134***
			(11.71)	(7.10)		(11.71)
MEAN_PERF			-0.166	-0.147*		-0.167
			(-1.74)	(-2.14)		(-1.76)
_cons	0.0440	0.0489	0.106*	0.113	-0.0587	0.0169
	(0.50)	(0.33)	(2.28)	(1.48)	(-0.30)	(0.15)
N	18907	18910	18907	18910	18907	18907
adj. R-sq	0.420	0.008	0.659	0.209	0.422	0.660

t statistics in parentheses
* p<0.05, ** p<0.01, *** p<0.001

Source: Stata Output

References

Salehi, M., Ghazanfari M., Fathian, M. (2017), *Data Mining Techniques for Anti Money Laundering*, International Journal of Applied Engineering Research

AIA Convention (1985), *Law applicable to trusts and on their recognition*

Barro, R. J., Jong-Wha Lee (2002), "*Education and Economic Growth*"

Bourdieu P. (1985), "*The forms of capital.*" In Handbook of Theory and Research for the Sociology of Education, ed. JG Richardson

Buonanno P., Montolio D., Vanin P. (2009), "*Does social capital reduce crime?"*, Quaderni di ricerca del Dipartimento di Scienze Economiche "Hyman P. Minsky", The Journal of Law and Economics

D.Lgs. n.267/2000

Directive (EU) 2015/849 of the European Parliament and of the Council

Ehrlich, I. (1975), "*On the Relation between Education and Crime*", Education, Income, And Human Behavior F. Thomas Juster, ed.

Bonaccorsi di Patti, E. (2009), "*Weak institutions and credit availability: the impact of crime on bank loans"*, Banca d'Italia Questioni di Economia e Finanza, page 11

EU Act (2002), "*Council Framework Decision of 13 June 2002 on combating terrorism"*

FAFT (1995), "*Annual Report 1994-1995"*

FATF *(*1997), *"Annual Report 1996-1997"*

FAFT (1998), "*Annual Report 1997-1998"*

FATF Guidance (2013), "*National Money Laundering and Terrorist Financing Risk Assessment"*

FATF (2003), "*Report on Money Laundering Typologies 2002-2003"*

FATF (2007), "*Money laundering and terrorist financing through the real estate sector"*

FATF (2008), "*Money Laundering and Terrorist Financing vulnerabilities of commercial websites and internet payment systems"*

FATF Report (2010), "*Money Laundering through Money Remittance and Currency Exchange Providers"*

FATF Report (2013), "*Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals"*

FATF Report (2013), "*The role of Hawala and other similar service providers in money laundering and terrorist financing"*

FATF Report (2015), "*Money Laundering Through the Physical Transportation of Cash"*

Reganati F., Oliva, M., (2017), "*The Determinant of Money Laundering: Evidence from Italian Regions"*, Department Digef, Sapienza, Rome, Italy, Economics and Financial Market freelance journalist, Rome, Italy

Fukuyama, F. (2000), "*Social capital and civil Society",* International Monetary Fund working paper

Venturini, G., Branchi, M. (2017), "*Il rapporto tra mafia e impresa: il caso della 'Ndrangheta nell'economia lombarda*", page 27

Groot, W. (2010), "*The effects of education on crime*", Article on applied Economics

Guiso, L., P. Sapienza, and L. Zingales (2004), "*The role of social capital in financial development*", American Economic Review, 94.

Helliwell, J. F., Putnam, R. D. (1995), "*Economic growth and social capital in Italy"*, Eastern Economic Journal, Vol. 21, No.3, Summer 1995

Helmy, T., Abd-ElMegied, M. Sobh, T., Badran, K. (2014), *Design of a Monitor for Detecting Money Laundering and Terrorist Financing*, International Journal of Computer Networks and Applications, Volume 1, Issue 1, November - December

http://dati.istat.it/Index.aspx?DataSetCode=INDUNIV#

http://siteresources.worldbank.org/EXTAML/Resources/396511114658142787 1/Reference_Guide_AMLCFT_2ndSupplement.pdf

http://www.comuniverso.it/index.cfm?Comuni_dal_1861&menu=12

http://www.finanze.gov.it/

http://www.unipd.it/ilbo/mafia-aziende-criminali-nord-italia

http://www1.finanze.gov.it/finanze3/pagina_dichiarazioni/dichiarazioni.php

https://elezionistorico.interno.gov.it

https://infostat.bancaditalia.it/

https://www.brocardi.it/codice-penale/libro-secondo/titolo-v/art416bis.html

https://www.interpol.int/Crime-areas/Financial-crime/Money-laundering

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3049417/

Le Mafie a Milano e nel Nord: aspetti sociali ed economici, Intervento del Governatore della Banca d'Italia, Mario Draghi, Milano, 11 marzo 2011

Madinger, J. (2011), "*Money Laundering: A Guide for Criminal Investigators, Third Edition"*

Fabrizi, M., Malaspina, P., Parbonetti, M., "*Caratteristiche e modalità di gestione delle aziende criminali"*, page. 2

McDonell, R. (1998), "*Money laundering methodologies and international and regional counter-measures,* National Crime Authority, NSW", paper presented at the Australian Institute of Research.

OECD (2019), *Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors*

Official website of the European Union, Migration and Home Affairs, "*Definition of Financial Intelligence Unit (FIU)"*, https://ec.europa.eu/home-affairs/e-library/glossary/financial-intelligence-unit-fiu-0_en

Schott, P. A. (2006), "*Reference Guide to Anti-money laundering and Combating the Financing of Terrorism (Second Edition)"*, Business and Economics

Reuter, P. Truman, E. M. (2004), *Chasing dirty money, the fight against money laundering, Institute for International Economics*

President's Commission on Organized Crime – Interim Report to the President and the Attorney General (1984), "*The cash connection: Organized Crime, Financial Institutions, and Money Laundering"*

Putnam, R. (1995), "*The Case of Missing Social Capital*", Harvard University working paper

Regulation (EU) 2015/847 of the European Parliament and of the Council

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014

Robert, M. Solow (2010), "*Stories about economics and technology*", The European Journal of the History of Economic Thought

Stamp, J., Walker, J. (2007), "*Money laundering in and through Australia, 2004"*, Trends & Issues in crime and criminal justice No. 342, Australian Institute of Criminology

Transcrime. 2013. "*Progetto PON Sicurezza 2007-2013: Gli investimenti delle mafie. Rapporto Linea 1.*" Milano: Ministero dell'Interno www.investimentioc.it

Venturini, G., Branchi, M. (2017), "*Il rapporto tra mafia e impresa: il caso della 'Ndrangheta nell'economia lombarda*"

World Bank (2006), *"Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism (second edition)"*