Vysoká škola ekonomická v Praze

Fakulta financí a účetnictví

katedra měnové teorie a politiky

studijní obor: Bankovnictví a pojišťovnictví

(Anti) Money laundering and its macroeconomic and microeconomic perspective

Autor diplomové práce: Bc. Diana Danková

Vedoucí diplomové práce: Ing. Ondřej Šíma

Rok obhajoby: 2017

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci na téma "(Anti) Money laundering and its macroeconomic and microeconomic perspective" vypracovala samostatně a veškerou použitou literaturu a další prameny jsem řádně označila a uvedla v přiloženém seznamu literatury.

V Praze dne ....

Bc. Diana Danková

Acknowledgements

I would like to express my deepest thanks of gratitude to my supervisor Ing. Ondřej Šíma for his help, invaluable advices and individual approach throughout the thesis work. Moreover, I would also like to thank to my mother who supported me a lot in finalizing this thesis within the limited time frame.

Abstract

The primary objective of this diploma thesis is to comprehensively present the issue of money laundering not only on a macro level but also in terms of commercial bank and its microeconomic response to it. The main contribution of this diploma thesis is to identify the global indicators, which should be considered when drafting strategies in the fight against the legalization of proceeds from crimes. This diploma thesis addresses the changes caused by current globalization and highlights the dangerous effects it has on evolution of this consequent criminal activity together with evaluation of its potential in the future. Due to the tense situation in Europe caused by the series of terrorist attacks, part of the work is dedicated to the explanation of the relationship between terrorist financing and money laundering.

Key words: shadow economy, money laundering, illicit funds, terrorist financing, AML/CTF policies, leading indicators

JEL classification: K14, O17, F51

Abstrakt

Cílem této diplomové práce je poskytnout čtenáři komplexní pochopení problematiky legalizace výnosu z trestné činnosti nejen z globální perspektivy, ale i z pohledu mikroekonomického, tedy především na úrovni jednotlivých bank. Hlavním přínosem diplomové práce je identifikace indikátorů, na které je třeba brát zřetel při koncipování strategií v boji proti této činnosti. Dalším přínosem je vysoká aktuálnost práce, která umožnila upozornit na rostoucí hrozbu této činnosti na virtuální úrovni a zhodnotit potenciál tohoto nového trendu. Vzhledem na vypjatou situaci v Evropě, kterou způsobila série teroristických útoků, je část práce dedikována i vysvětlení vztahu mezi financováním terorismu a „praním špinavých peněz“.

Klíčové slova: šedá ekonomika, legalizace výnosu z trestné činnosti, nelegální peněžní prostředky, financovaní terorismu, proti opatření, předstihové indikátory

JEL klasifikace: K14, O17, F51

Table of contents

List of abbreviations

AEOI - Automatic Exchange of Information

AML - Anti-money Laundering

AML/CTF - Anti-money Laundering/Counter-Terrorist Financing

BMPE - Black Market Peso Exchange

CDD - Customer Due Diligence

CIP - Customer Identification Program

CR - Czech Republic

CTF - Counter-Terrorist Financing

EC - European Commission

EU - European Union

FAU - Financial Analytical Unit

FATCA - Foreign Account Tax Compliance

FATF - Financial Act Task Force

FSI - Financial Secrecy Index

GAFILAT - Financial Action Task Force of Latin America

ICRG - International Cooperation Review Group

IMF - International Monetary Fund

IVTS - Informal Value Transfer Systems

KYC - Know Your Customer

ML - Money Laundering

MMORPG - Massively Multiplayer Online Role-Playing Game

NCCT - Non-Cooperative Countries and Territories

OECD - Organisation for Economic Cooperation and Development

OFAC - Office of Foreign Assets Control

OFC - Offshore Financial Centres

PEP - Politically Exposed Person

TF - Terrorist Financing

UBO - Ultimate Beneficial Owners

UK - United Kingdom

US - United States

UN - United Nations

Introduction

Creation of the international financial integrity was started off by globalisation that aided to breakdown the natural barriers that segregated domestic financial markets. Undoubtedly, not only benefited participants in the legal economy but also illegal economy exploited the vulnerabilities that came with it.

This diploma thesis attempts to approach the financial threat, specifically *money laundering*, which capitalized as one of the most on these newly formed opportunities. Its principle objective is to offer understanding of this global phenomenon from two different perspectives together with suggesting leading indicators that must be followed to eliminate this issue. Thus, it is divided into two imaginary parts, one dedicated to money laundering on international level and identifying leading indicators from global perspective, and the other grasped money laundering at a micro level highlighting leading indicators in terms of banking institutions.

The *first chapter* consists of several crucial elements. Only by approaching the matter of money laundering systematically, one can understand it clearly, without confusion. The crime is the very beginning, when the path of money laundering starts. This is the reason why it was rational to define the shadow economy and its principle characteristics at the outset. In the world of money laundering, it is paramount not to omit, that one can be accused of money laundering only when profit derives from the illicit activity that is considered a predicate offence. Thus, defining a clear and sufficient list of predicate offences should be of principle importance of any AML legislation. Additionally, money laundering is not only a threat because it enables criminals to enjoy profits with impunity but also for its adverse impact on real and financial sector of the economy.

Globalisation and digitalisation have alarmingly altered the way in which we live, communicate, and work but also the way in which criminals operate and launder their illegally obtained money. Cyber laundering, as the new generation of traditional money laundering, should not be underestimated neither by criminologists and economists nor by regulatory authorities. Online gambling, virtual currencies, prepaid cards are only a fraction of possibilities that cyber launderers misuse daily for their either latent regulation or simply

the nature that enables smoother and more sophisticated laundering. Therefore, the *second chapter* presents this growing menace and the dangerous potential it possesses.

Many still do not see the connection between money laundering and *terrorist financing* although it is nearly impossible to find the article, legislation or regulatory authority that does not incorporate terrorist financing together with money laundering. Terrorism has grown dramatically in recent years which is the reason why we consider it an inseparable part of this diploma thesis. Our main objective within the *third chapter* is to demonstrate that even though money laundering and financing of terrorism are basically two reverse actions, they share crucial commonalities that in the end brings them together.

Although there are no accurate approximations of the amount of laundered money, which is by the nature of this subject understandable, it is difficult for regulatory authorities to evaluate the outcome of their hard fight against this phenomenon. *The fourth chapter* aims at introducing the most powerful Anti-money laundering authorities and their centre of interest. The leading position certainly belongs to the Financial Act Task Force that created recommendations that grew into international standards adopted by many jurisdictions.

As we have outlined, measuring the amount of laundered money and obtaining some numbers almost always comes to a dead end. We strongly assume that identifying leading indicators in this industry can considerably aid in fighting and eliminating this undesirable element of any economy. Accordingly, we pick and identify certain indicators on global level and thus draw attention to the fact that money laundering must be also fight by eliminating the organized crime that creates it. Furthermore, since financial institutions have the greatest potential to be exploited by launderers and terrorists, we conclude this diploma thesis by presenting *certain Anti-money laundering measures on the example of Czech Republic* and by highlighting indicators that lead banks and financial institutions to the successful recognition of either attempted or undertaken suspicious transactions.

1 Money laundering

Money laundering (ML), the term that is well-known worldwide and troubles all economies, originates from USA describing the attempt of mafia to launder illicit funds through launderettes controlled by criminals in the early 30s.

This chapter aimed at providing, first, an essential understanding of what role shadow economy plays within this issue, as well as the definition and overview of ML process as such. Since ML represents a core problem of this diploma thesis, we attempted to clarify it in all its aspects. Irrespectively of such a complex issue, which it certainly is, we intended to provide its comprehensive interpretation.

1.1 The very beginning - shadow economy

"Black money is so much a part of our white economy, a tumour in the centre of the brain - try to remove it and you kill the patient."

Rohinton Mistry

The quote above expresses clearly that activities associated with shadow economies are simply part of life. The shadow economy hampers the public good by offering great benefits to certain individuals. Therefore, societies try to control these undesirable activities through many different means such as punishments, regulations, education or improving institutional framework. For its adverse effects, it is vital to gather as much information as possible about the extent of the shadow economy, its magnitude, who is engaged in these so-called underground activities, the source and the frequency of these activities.[1]

Not only measuring or gathering information about shadow economy is challenging but also defining shadow economy lacks a precise clarity. One of the broadest definitions and for our purposes the most suitable is following: *"…those economic activities and the income derived from them that circumvent or otherwise avoid government regulation, taxation or*

[1]SCHNEIDER, Friedrich. Shadow Economies All over the World. In:*www.worldbank.org* [online]. 2010 [cit. 2016-07-28]. Available from:https://openknowledge.worldbank.org/bitstream/handle/10986/3928/WPS5356.pdf?sequence=1

observation."[2] Our broad definition corresponds with a table given below that details various types of underground activities.

Table 1: Taxonomy of shadow economy activities

Activity	**Monetary transaction**		**Non-monetary transaction**	
Illegal	Trade in stolen goods; drug dealing and manufacturing; prostitution; gambling, smuggling, fraud, human trafficking …		Barter of drugs, stolen goods, production of drugs for own purposes …	
	Tax evasion	**Tax avoidance**	**Tax evasion**	**Tax avoidance**
Legal	Unreported earnings from self-employment; wages and salaries from unreported work…	Employee discounts; fringe benefits …	Barter of legal services and goods …	All do-it yourself work …

Source: Lippert, O., M. Walker (40)

From the previous text should be clear that shadow economy is a part of formal economy. The classification of shadow activities provided by table 1 comprises to imaginary axes. The horizontal axis differentiates monetary and non-monetary transactions and the vertical denotes the dichotomy between legal and illegal activities.[3] The underground economy includes all market-based legal production of goods and services that are designedly obscured from public authorities mainly for the following two reasons:

- To avoid payment of income, value added or other types of taxes.
- To avoid payment of social security contributions.

[2] SCHNEIDER, Friedrich. The Shadow Economy and Work in the Shadow: What Do We (Not) Know? In: *www.iza.org/en/webcontent/index_html* [online]. 2012 [cit. 2016-07-29]. Available from: http://ftp.iza.org/dp6423.pdf

[3] FOREST, James J. F. *Essentials of counterterrorism*. [e-book]. Santa Barbara, California: Praeger, an imprint of ABC-CLIO, LLC, 2015. ISBN 9781440834707. Available from: https://books.google.cz/books/about/Essentials_of_Counterterrorism.html?id=fcihCgAAQBAJ&redir_esc=y

There is number of literature that contributes largely to the issue of shadow economy and we believe that for our purposes, it is only sufficient to illuminate the linkage to ML. Firstly, it is beneficial to realize that the underground economy consists of at least two parts:

- Illegal sector that generates grey money.
- Criminal sector that generates dirty money (black money).[4]

Grey money derives mostly from tax evasion and thus includes for instance funds hidden in offshore centres. *Dirty money* refers to money gained from criminal activity such as drug trafficking or human trafficking, which is associated with much severe penalties. This implies that there is a slight difference between grey and dirty money but what brings them together is that both evoke ML.[5]

One can still ask why there was need to specify shadow economy in context of ML. To provide a real and complex understanding of ML, one must start from scratch. At the beginning of every laundering scheme, there is any kind of illicit activity that generates illegally tainted money. To safely operate with this profit, without being detected, premeditated ML process must be designated and successfully conducted so the taint is removed. Therefore, unsurprisingly, ML functions as a connection between formal and informal economy, as it enables the flow of resources between them. Besides, it is crucial not to omit, that ML is not a cause of shadow economy but a *manifestation* of it. Namely, dirty or grey money is worthless, as it leaves behind a trail of incriminating evidence.

In the previous text, we have intentionally simplified the problem of ML and shadow economy in order to underline the linkage between them. We have assumed that all types of criminal activities belong to ML. However, realistically speaking, we are bound to the countries legislation. One can be accused of ML only if the crime is on the list of predicate offences. The separate subchapter was dedicated to the deeper clarification of this issue in the following text.

[4] HINTERSEER, Kris. *Criminal finance: the political economy of money laundering in a comparative legal context*. [e-book] Boston, Mass.: Kluwer Law International, 2002. ISBN 9041198644. Available from: https://books.google.cz/books/about/Criminal_Finance_The_Political_Economy_o.html?id=Cx3x4EijpXsC&redir_esc=y

[5] *Gray Money* [online]. [cit. 2016-07-29]. Available from: http://financial-dictionary.thefreedictionary.com/Gray+Money

1.2 Definition and overview of the process

Having introduced ML within the first subchapter without specifying it in detail was intentional, but necessary to grasp this complex issue from the very beginning.

The term ML is ambiguous, more than anyone would expect. Finally, ML is a sophisticated crime that can be defined as a legitimization of illegally gained money with aim of hiding its true source or nature. That is to say, it is the process of creating appearance that certain amount of money obtained from underground activities originates from legitimate source.[6] This complex process is of prime importance, as it enables criminals to enjoy their profits without jeopardizing their source.

When a crime occurs, and is successful, it obviously generates a great amount of profit, so individuals interested in it must find a way to put these funds under control, avoiding attention of authorities. They do this by erasing the link between the crime and the money and ultimately erasing the link between the money and new owner. Differently, they cannot use their proceeds of crime (or can, but it would easily connect them to the illegal activity) without the legitimization. There is a common misperception that ML happens only in connection with drug trafficking but it must be borne in mind that, simply put, any money or benefit resulting from illegal activity is considered proceeds of crime and can be a subject of ML.

Generally, there are three steps involved in the process of ML. This creates a perception that it is a very complex process. It certainly is true but by dividing it into three phases one can better understand the process, realize the importance of each phase and see the nexus between them. For better imagination, we provide a few brief examples of how the stage can be done. Remember that some techniques may be applicable for each stage.

[6] *Money Laundering* [online]. [cit. 2016-07-29]. Available from: http://www.investopedia.com/terms/m/moneylaundering.asp

ML can be then viewed as a dynamic process that takes place in three stages:

1. Placement represents the initial injection of proceeds of crime into the legitimate financial system. We may say that this stage serves two purposes:

- The launderer can relieve of keeping a mountain of cash and change the money into a more portable and less suspicious form.
- Through the placement stage, the illicit funds are integrated into the legal financial system.

Because placing the large amount of cash into the financial system is suspicious (or should be), placement stage might be very vulnerable. As most of the illegal activities generate proceeds in cash, the launderers can be easily caught at the outset. There are many ways through which the process of placement can be carried out:

- *Smurfing* is probably the most common placement technique. It is very popular among launderers and likely still much executed. This technique aims at reducing the large susceptible volume of money by dividing it between deposit specialists (smurfs) that consequently deposit the money into the banks and other financial institutions without fear of detection.
- *Currency smuggling* is a physical movement of currency across the border. Development of electronic money reduces the need for currency smuggling because electronic money is easy to transfer and its characteristics highly attract money launderers. Despite of that, currency smuggling is still not out of date and currency remains fundamental form of illegal proceeds.
- *Bank complicity* is a situation when bank or other financial institutions is controlled by individuals willing to undertake underground activities and cooperate with drug dealers and other organized crime groups.
- *A currency exchange* is nothing but purchasing foreign currencies with illegally obtained funds. Liberalization of foreign exchange markets enables such a currency movements and makes it feasible for money launderers.
- *Securities brokers* can represent a mean of facilitating ML process through structuring a large amount of cash in a manner that conceals its origin.
- *Blending of funds* signifies hiding cash with many other cash and thus financial institutions are the best vehicles.

- *Asset purchase* is a standard ML technique with the purpose of transforming the proceeds of crime to certain equally valuable form.[7]

2. Layering is another stage focused on making it more difficult to detect the origin of "dirty money". Put differently, it includes the separation of illegal proceeds from its source by using complex layers of financial transactions with intention to disguise the origin. This stage can be carried out by moving money electronically from one jurisdiction to another, consequently dividing the funds into the great deal of transactions always harnessing the loopholes and possible disparities. Their constant move aids to elude the detection or make it much harder to track it down.[8] As an example, following two methods can be given:

- *Cash converted to monetary instruments.* As soon as the stage of placement is done and illicit funds are placed into financial systems, the proceeds can be transformed into monetary instruments (money orders, banker's drafts).
- *Material assets bought with cash, then sold.* Assets that are purchased from proceeds can be resold which creates confusion. In this case, the assets become more difficult to trace and thus seize.[9]

With the advent of complex financial transactions, financial derivatives are commonly used in this stage. To understand better the misuse of financial derivatives, we can imagine two offshore companies that are "de iure" separated, but "de facto" administered by one person. They may then easily arrange an option contract with one another, by taking short and long positions. Naturally, the loss of one subject is compensated by the profit of the other one.

It is called layering stage because generally, the transactions conducted in this phase form a layered construction. Otherwise stated, they are executed in a sequential manner, which means that one transaction is stacked on the top of the other one. Layering depends on a several aspects. It can be assumed that if the layering transactions cross certain number of national boarders (physically or electronically), it increases the chance of a successful

[7]*Money Laundering in the EU: Methods and Stages of Money Laundering* [online]. [cit. 2016-07-30]. Available from: http://people.exeter.ac.uk/watupman/undergrad/ron/methods%20and%20stages.htm
[8]*Money Laundering: A three-stage process* [online]. [cit. 2016-07-30]. Available from: https://www.moneylaundering.ca/public/law/3_stages_ML.php
[9]Ibid. (7)

realization. This is the reason why layering phase usually involves two or more jurisdictions.[10]

3. Integration, as a final stage, converts illegally obtained funds into apparently legitimate earnings through financial operations. Integration is mainly undertaken through banking system and this is finally the stage where the money returns to the criminal from what seems to be a legitimate source. It is crucial to reunite the money with the individual in a way that does not draw attention and it is not suspicious. Needless to say, the integration is a culmination of a successful ML as the proceeds become available for the criminal. The money can be then used for personal benefits. Two following techniques can be used in the integration phase:

- *Real estate* is a well-known harbour for launderers. As the properties are non-depreciating assets worldwide, this choice is no surprise. This situation requires an agent that neglects the fact that launderer pays with a bulk of cash. As we will see later, this can commonly happen also in well-developed countries.
- *Capital investments* can be used in all stages. Capital market may be used for an initial injection of illicit funds to the financial system. In addition, it can be used in layering phase because capital investments offer many possibilities for transactions of different types. No one can argue that capital investments might also be a final choice for launderers, or in other words, their final destination. If the launderer chooses a low-risk investment, such as bonds, the chance of losing the money is also low. The benefit of this choice certainly lays in its liquidity compared to real estate investments. [11]

To conclude this subchapter, it should be noted that the aforementioned stages do not necessarily exist in the mind of a launderer and he or she certainly does not think about it this way. These stages are to some extent generalization based on the experiences of investigators and regulatory authorities. Moreover, they do not have to follow a linear pattern and the process may not even include all stages. The stages can even flow into each other

[10]RICHARDS, James R. *Transnational criminal organizations, cybercrime, and money laundering: a handbook for law enforcement officers, auditors, and financial investigators*. [e-book].Boca Raton, FL: CRC c1999. ISBN 0849328063. Available from:https://books.google.cz/books/about/Transnational_Criminal_Organizations

[11]MASCIANDARO, Donato. TAKÁTS, Elöd. UNGER, Brigitte. *Black Finance: The Economics of Money Laundering*. Cheltenham (UK): Edward Elgar, 2007. ISBN 10-1782543473

and create an overlap between them. Therefore, it is not relevant for investigators to indicate on which date a certain phase happened. Distinguishing between stages is mainly to understand the process and recognize a certain transaction as being part of such a scheme. This implies that investigators should not be blinkered by this traditional pattern of ML.

1.3 Predicate offences

Predicate offence is simply an offence generating proceeds that can be subject of ML. What is not that straightforward is the fact that there are many variations of what is included under the list of predicate offences and what is not.[12] This varies from state to state and thus we have focused merely on the approach of European Union (EU) towards this issue. Let us remind that individual can be persecuted from ML only if the crime from which the profit is derived is included under the predicate offences.

EU Directives constitute the legal base of Anti-money laundering (AML) regulation and are legally binding given the achieved aim no matter what forms and methods are used. Evolution of these Directives, including all-important amendments, is presented in more detail in chapter 4. At this point, only amendments regarding predicate offences were relevant for us.

ML, as a crime, attracted attention in 80s mainly regarding drug trafficking. This implies that initially, crimes regarding drugs were included under the predicate offences. This also confirms the text of the first AML Directive from 1991 concerning only proceeds of drug trafficking. Despite the second Directive adopted broader definition of ML, covering all serious offences such as corruption or fraud, the Member States were permitted to include any other offences which consequently led to an uneven coverage across the Europe. The third Directive increased in scope as well, considering revision of the Financial Act Task Force (FATF)[13] requirements from 2003 and thus including terrorism among predicate crimes. Specifically, predicate crimes encapsulated:

- Terrorism**.**

[12] Criminalizing the laundering of proceeds of trafficking in persons. *Https://www.unodc.org/* [online]. [cit. 2016-08-02]. Available from: https://www.unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_3-5.pdf

[13]The FATF is a multinational regulatory authority that sets up international standards within ML/TF. Its vital role is discussed later in the chapter regarding combating ML/TF.

- Drug offences.
- Activities of criminal organizations.
- Serious fraud and corruption.
- Other crimes determined nationally.
- All other offences that are punishable by a long period of imprisonment.[14]

The latest revision of the FATF recommendations in 2012 has again expanded the scope of predicate crimes to include tax crimes. As is customary, EU considered this revision and as a result, the fourth AML Directive has expanded its scope too, including tax crimes and reinforcing the relationship between AML and Tax authorities.[15] The Directive does not provide a specific definition for which offences would amount to a "tax crimes" so it will be up to Member States to specify it within their national legislation.

1.4 Impact of Money laundering on the economy

In previous chapters, we have tended to accentuate the menace of ML as it has become a global phenomenon taking place worldwide. It is certainly not comfortable to admit that ML undermines economies and constitutes the threat to the governments.

By the nature of the subject, it is nearly impossible to measure the amount of illicit activities, but despite of that, there were several attempts to quantify the volume of laundered money. Estimation shows that almost 2 to 5 % of global gross domestic product is laundered each year.[16] The spread indicates that it is extremely difficult to estimate it but even if we took the minimal estimation, it would still demonstrate the seriousness of this global phenomenon and its force. With that being said, we have attempted to clarify the adverse effects of ML on both financial and real sector.

Financial sector

Several studies have been undertaken to evaluate the contribution of financial institution in economic development and all studies have reached the same decision: sound domestic

[14]SPARKES, Peter. *European land law*. [e-book]. Portland, Or.: Hart, 2007. ISBN 1841137588. Available from: https://books.google.cz/books/about/European_Land_Law.html?id=3e7bBAAAQBAJ&redir_esc=y

[16]Money-Laundering and Globalization. *United Nations office on Drugs and Crime* [online]. [cit. 2016-08-11]. Available from: https://www.unodc.org/unodc/en/money-laundering/globalization.html

financial sector is of critical importance. The essential role that banks, non-banking institutions or equity market play in economic growth is provided through their function in capital formation and allocation.[17] Financial sector, including banking and non-banking institution, is especially vulnerable to ML. Financial institutions can play three basic roles in financial crimes:

- Victim.
- Perpetrator.
- Instrumentality.

The third category is a centre of our interest because here is where financial institutions are misused to keep or transfer illicit funds, knowingly or not. Needless to say, the third category is mostly represented by ML.[18] As financial institutions are particularly susceptible, we can summarize that ML weakens the sustainability and development of financial institution in two fundamental ways:

- First of all, financial institutions are harmed directly as there seems to be an obvious correlation between ML and fraudulent activities carried out by employees. Consequently, it strengthens the criminal activities and other parallel system of ML channels.[19]
- Good reputation builds customer's trust that is primary for the sound financial system. Hence, the significance of confidence and the need of transparency in the financial system should not be de-emphasized, principally as it makes a considerable contribution to certain countries' gross national product. [20]

Globalization and current efforts in complete financial market integration unwittingly facilitate the financial abuse, causing cross border negative externalities. As trust underpins the development and existence of financial institutions, ML as a form of financial abuse, can weaken the financial systems. To be more concrete, abuse of financial sector can yield to

[17]The role of financial markets for economic growth. *ECB* [online]. [cit. 2016-08-11]. Available from: https://www.ecb.europa.eu/press/key/date/2001/html/sp010531.en.html
[18]Financial System Abuse, Financial Crime and Money Laundering. *IMF* [online]. 2001 [cit. 2016-08-12]. Available from: https://www.imf.org/external/np/ml/2001/eng/021201.pdf
[19]KUMAR, Vandana. Money Laundering: Concept, Significance and its Impact. In: *European Journal of Business and Management* [online]. 2012 [cit. 2016-08-14]. ISSN 2222-2839. Available from: http://www.iiste.org/Journals/index.php/EJBM/article/view/1040/960
[20]KEHOE, Mark. *The threat of Money Laundering* [online]. In: . 1996 [cit. 2016-08-14]. Available from: http://econserv2.bess.tcd.ie/SER/1996/mkehoe.htm Tanzi, Vito. 1999. Uses and Abuses of the Estimates of The Underground Economy. Economic Journal 109:338-47. Available from: https://www.jstor.org/stable/2566007?seq=1#page_scan_tab_contents

potential large fiscal liabilities on the side of financial institutions, increase the volatility of capital flows on the international level and enhance exchange rates volatility.

The large capital inflows and outflows undertaken to legitimize ill-gotten funds detrimentally affect exchange rates, interest rates, and thus essentially influencing the process of particular assets towards which the money is put. As a result of unhampered fluctuation of exchange rate, the huge inflow of capital then leads to the appreciation and an expansion of the country's money base. This will subsequently result in increase of the demand of domestic money with adverse impact on export as it loses competitiveness to the import.[21] The above effect is surely to some extent speculative and in absence of hard statistical data unable to be demonstrated. However, given the fact that ML is taking place on a large scale, it cannot be ruled out and thus macroeconomic policy makers should consider it. Again, these activities are concealed and therefore monitoring by macroeconomists and statistics is impossible. Moreover, to identify the country and the currency of issuance and ultimately the residency of deposit holders is key and stumbling block. What we can conclude is that to the extent that money demand seems to move from one country to another as a result of ML, leading to deceptive monetary data, it will have unfavourable consequences for interest and exchange rate volatility.[22]

Allegations can have far-reaching consequences and can greatly affect reputation of a country. This consequently affects the willingness of foreign investors and financial institutions to conduct businesses in that country. This has also considerable effect on correspondent banking relationships. Correspondent banking network has an irreplaceable role in supporting trade ties between countries and banks are very careful with what bank (jurisdiction) they are dealing with as part of their AML policy.

Real sector

Negative effect on real sectors lies in the fact that ML diverts resources to the less productive activities. To understand this, we need to realize that flow of illicit funding follows a path across the economy that is diverse than such funds would take if they did not have to be

[21]Tanzi, Vito. 1999. *Uses and Abuses of the Estimates of The Underground Economy.* [online]. 1999 [cit. 2016-11-03]. Economic Journal 109:338-47. Available from: https://www.jstor.org/stable/2566007?seq=1#page_scan_tab_contents

[22]QUIRK, Peter. Money Laundering: Muddying the Macroeconomy. In: *IMF* [online]. Washington, 1997 [cit. 2016-08-14]. Available from: https://www.imf.org/external/pubs/ft/fandd/1997/03/pdf/quirk.pdf

legitimized. Why? Because money launderers are in general not interested in maximizing the value of their funds, but rather in protecting them. As ML has been part of the economy over decades, some of the methods are well-known so it is nothing new that "sterile" investments function as harbours for illicit funds. The problem is that these investments do not generate extra productivity for the economy. The best example for a "sterile" investment can be a real estate. Properties are one of the most targeted assets because of their advantageous characteristics:

- It is a safe investment that holds its value.[23]
- The possibility to pay in cash is very useful as criminal activities mostly yield cash.
- The objective value is difficult to evaluate.
- It enables to realize "white" returns.[24]

Other preferred possessions are works of art, jewellery, luxury assets, etc. Productive enterprises transformed into sterile investments whose only purpose of existence is to launder illicit proceeds, not to maximize profit and contribute to a market competition is another great illustration. In consideration of foregoing, this ultimately reduces the productivity of the entire economy. There is another significant consequence. As real estates are often favoured among other assets, higher demand eventually drives the prices up causing overpayment and distortions in the resource allocation process. Once again, these activities are not possible to quantify but considering the magnitude of ML, the correlation must exist.[25] Observing the abnormal prices movements might seem to be a promising way to estimate ML, at least in this sector. On the other hand, this certainly has its limitations and such estimation encounters a fundamental obstacle: the fluctuations can be simply caused by pure speculation.

For the better illustration, we can demonstrate this problem on the example of United Kingdom (UK). Ownership of London properties via offshore companies has helped significantly to shape the real estate market where prices have risen up to 50 % since the year of 2007. Overseas companies based in offshore tax havens own approximately 100 000 estates in UK. Owning a property by using a shell company offers anonymity, a critical need

[23]When we abstract from price bubble.
[24]Money laundering through real estate. *Australian Government* [online]. [cit. 2016-08-14]. Available from: https://www.innanrikisraduneyti.is/media/peningathvaetti/MoneyLaunderingThroughRealEstate.pdf
[25]Countering Money Laundering and the Financing of Terrorism. *Asian Development Bank* [online]. 2003 [cit. 2016-08-14]. Available from: https://www.unodc.org/tldb/pdf/Asian-bank-guide.pdf

for successful ML, and what is more, helps easily bypass AML checks. Furthermore, in 2015, there were more than 1,2 million property transactions that generated only 355 suspicious activity reports which is alarmingly small number given the fact that real estate is a safe haven for ML, not to mention the UK situation that we have outlined.[26]

Another actual example, as this topic certainly deserves more attention, is situation in Vancouver, Canada. According to the Financial Transactions and Reports Analysis Centre, real estate firms in Vancouver do not comply sufficiently with AML obligations that require to identify the clients and from where their money comes. These deficiencies aid greatly to launder illicit funds through this vulnerable market. Moreover, these firms do not report suspicious transactions or large cash payments even though they are obligated to do so. To confirm this worrisome situation, between 2012 and 2015, the mentioned agency received only 7 questionable transactions.[27] Prices of the detached houses in Vancouver have risen by 37 % over last year. Because of this rapid growth and the fact that housing prices in other provinces (British Colombia, Ontario) have been rising steadily, there are speculations that a real estate market in Vancouver is fuelled by a ML bubble.

As the firms create the core of a real economy, it would not be appropriate to leave them out. As we have highlighted previously, front companies or shell companies are a well-known laundering method. It is they that cause the most serious microeconomic issues. Since these companies have subsidized funding, they are able to offer their products or services at below-market prices. This provides them with a competitive advantage over the legal businesses. As a result, legal businesses are unable to compete against these entities whose only purpose of existence is to protect illegal proceeds. In extreme cases, not that extreme in developing countries, ML proceeds can be used to control whole industries what then leads to a monetary or economic instability because the allocation of resources is disrupted.

To conclude this chapter, it is paramount not to omit that ML brings also significant social costs. Successful ML strengthens next activities of criminals and enables them to expand

[26]London property market turned into money laundering safe haven by inadequate supervision. *www.independent.co.uk* [online]. 2016 [cit. 2016-08-14]. Available from: http://www.independent.co.uk/news/business/news/london-property-market-real-estate-money-laundering-overseas-foreign-buyers-mps-a7138176.html

[27]Vancouver housing market 'vulnerable' to money laundering. *www.theglobeandmail.com* [online]. 2016 [cit. 2016-08-15]. Available from: http://www.theglobeandmail.com/news/national/vancouver-housing-market-vulnerable-to-money-laundering/article29285770/

their operations and certainly improve their methods and move their ideas to the next level. In this regards, governments must respond by reinforcing laws and changing counter measures not to lag behind innovative ideas of criminals. Unfortunately, these reactions drive up the costs, not to mention that also health care expenditures might considerably increase because of needed treatment of drugs addicts. In addition, ML reduces government tax revenue that indirectly harms other taxpayers. Increased costs on the side of public sector might then lead to the increased tax burden, which will certainly meet with the negative respond of population.

Adverse effects of ML on economic development are clear but also difficult to quantify. This financial crime damages the financial institutions that no one can doubt are absolutely critical for the thriving economy and reduces productivity in the real sector by encouragement of crimes and corruptions. Since the current aim is to integrate financial markets, any jurisdiction involved in the international financial system is vulnerable and expose to the risk of ML.

1.5 Informal value transfer systems

We believe that if we aim to provide a comprehensive overview of ML, the informal value transfer systems (IVTSs) cannot be omitted. IVTSs operate outside the conventional financial system, where either value or funds are transferred from one geographic location to another and their importance in ML industry is vital given the fact that it appears unfeasible to try to stop or eliminate them.

The legitimate use of IVTSs, such as humanitarian or emergency aid to geographic regions where financial infrastructure is either weak or absent, should not be ignored. On the other hand, vulnerabilities with regard to possible abuse, underestimated. Many systems move funds or value from place to place on behalf of terrorists or criminal organizations, successfully leaving almost no trace. Within this chapter, we have focused merely on two of them:

- The Black HAWALA.
- The Black Exchange Peso Market.

1.5.1 The Black HAWALA

HAWALA system was established in India long before the West banking system was developed in its present form and it is associated mostly with South Asia, Middle East, North Africa and Horn of Africa. It can be easily described as remittance system running in parallel with traditional banking and thus, it is often referred to as "underground banking". To transfer money, it often uses "non-business" relationships, such as family or religion. Notwithstanding the importance of family connections, it is primarily a business contributing in some extent to informal economy and this is how it should be mainly perceived.[28]

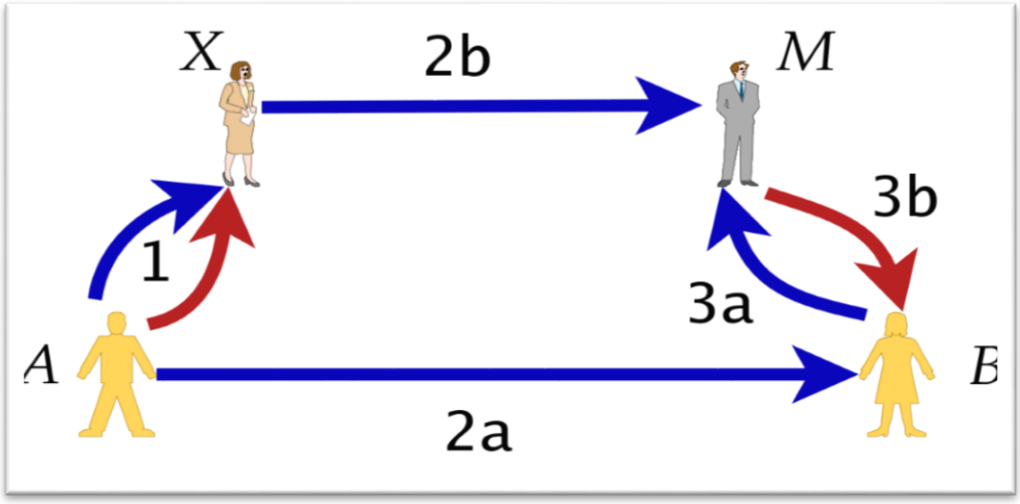
Its mechanism can be summarized as transferring money without actually moving it. To have at least elementary grasp of the system, let us explain how the transfer is carried out:

- A customer, recipient A, that for whatever reasons does not desire to use services of a regulated bank merchants, approaches HAWALA broker X and gives him money. There is no written contract for this transaction. This sum of money is to be transferred to a recipient B who usually is located abroad. Together with money, he specifies something like a password that will consequently lead to the money being paid out (red and blue arrow 1 on picture 1).
- The recipient B is naturally also informed about the password (blue arrow 2b).
- In the next step, HAWALA broker X calls HAWALA broker M informing him about the password and other necessary instructions (blue arrow 2b). At this point, an informal debt is created, which will be settled at a later date. Family, or kinship ties are highly used here and aid to ensure the future settlement.
- The recipient B can now approach HAWALA broker M with the password (blue arrow 3a). If the password is correct, HAWALA broker M can pay out the funds, obviously, reduced by a small commission (red arrow 3b).

Since the "transfer" runs under the rule of honor system, which means it is not based on strictly enforced rules, broker M has to trust to broker X to settle the debt. Besides, no promissory documents are exchanged between them.

[28]THOMPSON, Edwina. The nexus of drug trafficking and Hawala in Afghanistan. In: *www.worldbank.org* [online]. [cit. 2016-08-08]. Available from: http://siteresources.worldbank.org/SOUTHASIAEXT/Resources/Publications/448813-1164651372704/UNDC_Ch6.pdf

Picture 1: Transfer within HAWALA system



Source: www.explainbetter.wordpress.com (84)

HAWALA system surely is very vulnerable mainly because it is based on trust. Despite of that, certain individuals are motivated to use HAWALA system rather than traditional means of remitting money because of its following features:

- Cost effectiveness.
- Efficiency.
- Lack of bureaucracy and record keeping.
- Tax evasion.[29]

Again, migrants or poor people can use HAWALA for completely legitimate purposes, but aforementioned advantages indicate that it possesses features very vulnerable to abuse and thus serves perfectly for ML intensions. To differentiate legal and illegal HAWALA, the term "Black HAWALA" is usually used. Criminals highly appraise that customer identification performed by HAWALA brokers is not that rigorous (if at all). Due to this, it is far easier to transfer illicit money through these kinds of systems. We have outlined that there is no or very little record keeping what impedes any investigation activities at the outset. Even if records are available, they are often falsified what keeps them unobservable.[30]

We have introduced all three stages of ML in the previous chapter and therefore now, we will be able to apply them and illustrate how HAWALA can be used in each of these stages.

[29]Given advantages may also be observed in other remittance systems, not only in HAWALA.
[30]The role of Hawala in ML and TF. *FATF* [online]. [cit. 2016-08-08]. Available from: https://www.imolin.org/pdf/imolin/Role-of-hawala-and-similar-in-ml-tf-1.pdf

First of all, HAWALA can be very conducive in placement stage. In our illustration, the recipient received, let us say 6 000 €. Since we can suppose that recipient also runs a legitimate business, he will make a periodic deposit to the bank and justify it as proceeds of a legitimately running business. Besides, recipient can use some of the cash to pay the business expenses. The key in layering stage is to create as complex web of transactions as it is possible. The traditional banking system makes this stage very vulnerable because the transaction can easily arouse suspicion and in worst-case scenario (for launderer) lead investigators directly to the source of illegal funds, destroying both the laundering attempt and criminal cell. HAWALA systems leave behind very confusing paper trail, if any, what completely impedes any investigation activities. There were several research activities concerning HAWALA and its role in ML and it was revealed that even the simplest transfers are very difficult to trace down. With that said, using HAWALA brokers in number of countries and distributing the transfers of funds over time creates a perfect layering stage with minimal chance of detection and facilitates the development of international ML. Integration stage can also benefit from HAWALA features. This stage provides a legitimate-appearing explanation for the funds. HAWALA techniques are able to transform money into many different forms and thus creating possibilities for establishing their legal appearance. With this in mind, HAWALA system is not only about ML. It was revealed that Al Qaeda used HAWALA for transferring funds when planning terrorist attacks. Therefore, it is very plausible that other terrorist groups harness these systems too. In fact, in the aftermath of 9/11, the growing concern about these systems has culminated.[31]

HAWALA system is not illegal per se and each country has taken individual position regarding its legal status. The scale of unregulated HAWALA is unknown and it is not easy to obtain some credible estimates. This, together with the fact that unregulated operators are very vulnerable to ML/TF risks, makes HAWALA systems accessible for abuse.[32] Regulatory authorities deal with alternative remittance systems and their potential abuse due to their anonymity and other key attributes. As a result, International Monetary Fund (IMF) encourages following two approaches:

[31]JOST, Patrick. The Hawala alternative remittance system and its role in ML. In: *United States Department of the Treasury* [online]. [cit. 2016-08-08]. Available from: https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/FinCEN-HAWALA-rpt.pdf
[32]Ibid. (31)

- In jurisdiction where HAWALA-like systems operates alongside a traditional banking channel, HAWALA brokers should be registered and appropriate record keeping trails should be ensured as well. Considerable emphasis, to improve transparency level, is recommended too.
- At the same time, the regulatory response should address weaknesses and deficiencies that may occur in the formal sector.

The question regarding regulation of HAWALA systems is contradictory. On the one hand, it is undoubted that criminals make extensive use of it, on the other, too strict regulation can totally deprive poor people from legal sources of income and endanger their survival. This is much broader issue. Consequently, necessary balance is hardly achievable.

1.5.2 The Black Market Peso Exchange

Trade-based ML techniques are amongst most common laundering techniques criminals use to move money and clean them without detection. To outline HAWALA without mentioning the Black Market Peso Exchange (BMPE) would surely be unbalanced. It is also an essential vehicle for ML, especially used by Colombia drug traffickers in repatriating revenues to Colombia. It is believed to be the single most effective and extensive ML scheme in the Western Hemisphere. The BMPE was not created primary as a ML tool, just like HAWALA. There were two things that Colombian government did that led to the creation of this system. Firstly, they banned the United States (US) dollar and established very high tariffs on imported goods. The reason was to strengthen the value of peso and to increase the demand for Colombian goods. This all served to facilitate the growth of underground economy. More simply put, it constituted a black market exchange system where pesos are exchanged on the streets for dollars on deposit in American financial institutions to circumvent restrictive policies on currency exchange. Finally, yet importantly, this technique can be used with *any currency*, but since it was created in Latin America, it is mostly associated with pesos.

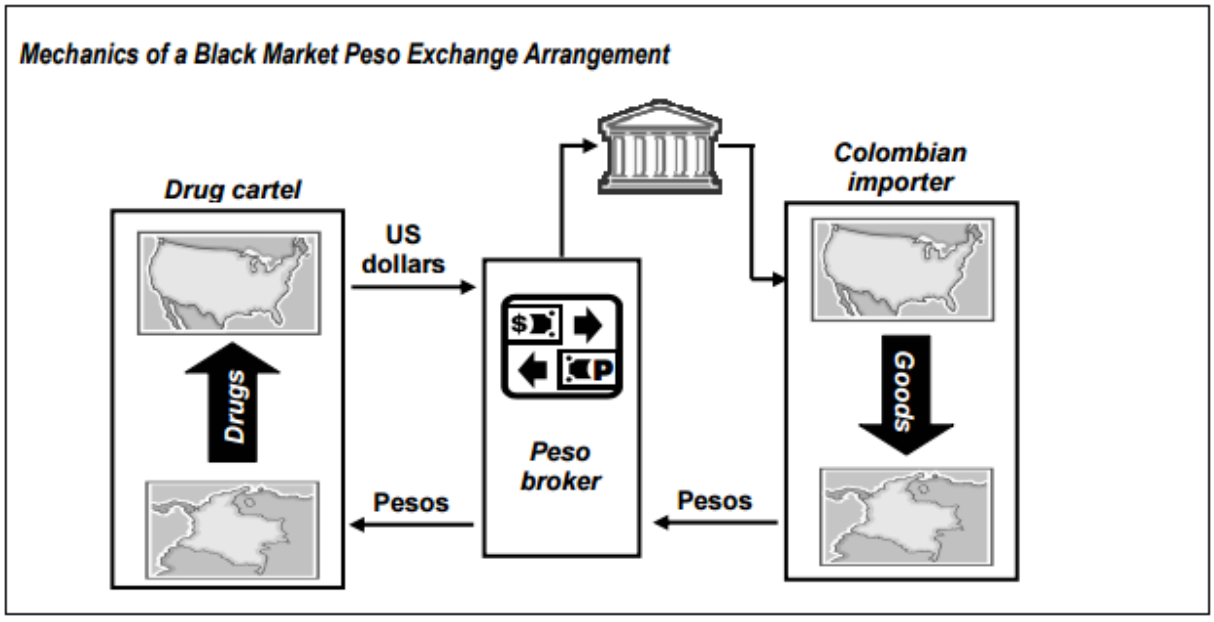
At this point, we might easily structure ML transaction with the use of BMPE. For better understanding, it is detailed on picture 2:

- Narcotic traffickers sell drugs in the US in exchange for dollars.
- Consequently, drug cells sell these dollars to a peso broker at discount over official rates in exchange for pesos. The peso broker, known also as cambista, is a money

broker with connections and bank accounts in financial institutions, on both sides of the border. The broker pays them from its bank account in the home country.

- The broker structures deposits of dollars into the broker's affiliated US bank accounts, known also as funnel accounts, to avoid reporting requirements of the US Bank Secrecy Act.
- The broker locates importers in the broker's home country that import goods from the US and need dollars to pay their US suppliers.
- The broker arranges to pay these suppliers on behalf of the importer in dollars from the funnel account in the US. Upon receipt of the US dollar funds, the US supplier exports the goods to the country of the importer.
- Ultimately, the importer, upon receiving the goods, sells them in the home country and pays the broker the arranged exchange fee in pesos, depositing them into the broker's local account. This refills the broker's bank account with local currency with which the broker can initiate a new trade-based ML transaction.

Picture 2: Mechanism of BMPE



Source: The FATF (17)

The mechanism of the BMPE is again simple. On the other hand, the networking involved might be exceptionally complex. Like the HAWALA, the BMPE is a sort of "honor system" that works, and continues to work this way. However, they both serve to launder illegal profits, they are not illegal per se.

2 Cyber laundering as a new Money laundering ?

"Electronic money laundering will boom, traditional paths are already highly supervised."

Dr. James Backhouse

Unfortunately, as the quote demonstrates, ML has evolved in the past years. ML is a living process that must respond to new emerging countermeasures and change its tactics if it wants to survive. Innovations, in terms of modern technologies and globalization, with regard to growing importance of Internet, have given rise to a completely new range of sophisticated techniques. The old methods of ML certainly exist, but as these methods have been well-known for decades, they have logically become very vulnerable, in terms of being detected at the outset. The gradual development of technologies and increasing significance of Internet have constituted a solution to many aspects of life and made things easier to happen, including ML. As they say, everything good can be abused or misused. There is no doubt that cyber laundering has evolved with the advent of Internet.

The term cyber laundering can be viewed as *"utilizing Internet-based electronic wire transfer methods, such as Internet banking or online gambling, in furtherance of disguising the source of illegally obtained money."*[33] This implies that objective of the process remains the same, but the method to do so has evolved. Notwithstanding the fact that there are only a few cases of cyber laundering, assumption that there is no cyber laundering would be naïve. Why is it so? The money launderers always look for a way to launder their proceeds of crime that meets all the following criteria:

- Quick.
- Discrete.
- Secure.
- Global.[34]

[33]WILLIAM H. BYRNES, ROBERT J. MUNRO., William H. Byrnes, Robert J. Munro. *Money laundering, asset forfeiture and recovery, and compliance: a global guide*. [e-book]. 2011. ISBN 9780327170846. Available from: https://books.google.cz/books/about/Money_Laundering_Asset_Forfeiture_and_Re.html?id=cVLUdo4JQv4C&redir_esc=y

[34]STRAUSS, Kilian. How can we effectively combat the use of the Internet for money laundering? In: *Kilian Strauss* [online]. [cit. 2016-08-20]. Available from: http://www.academia.edu/1369342/Cyber laundering_-_How_can_we_combat_money_laundering_over_the_Internet

If we evaluated traditional ML techniques, we are sure that none of them would make the grade. However, if we get back to the Internet, we quickly find out that it meets all these conditions. There is also no secret that terrorists use Internet as a mean of communication, to spread propaganda or to raise funds. Both criminals and terrorists are becoming cyber-savvy, which enables them to take advantage of the above-mentioned benefits and unlimited possibilities that Internet offers. To successfully combat cyber laundering, we should first understand how it works.

2.1 Process of cyber laundering

In essence, cyber laundering is another non-traditional method of ML. To understand its functioning, we can help ourselves with the well-known three-phased model.

Placement is the first stage where launderers benefit from the anonymity of Internet transactions. The ways by which the placement phase can be carried out in terms of cyber laundering are following:

- Deposit the cash through non-regulated institution.
- Deposit the cash with the help of smurfs through deposit automated teller machine (ATM).

Layering is the phase where the benefits of the Internet can be grasped entirely. If launderers find institutions, such as online casino, that allows creating an account without identification, it will be almost impossible for authorities to track this activity down. In addition, Internet offers almost immediate transmission of money which requires only Internet accessibility, not to mention that online bank transfers are hard to track back as a result of disguised Internet protocol adresses. [35]

The stage of **integration** can also benefit from cyber laundering advantages. There are number of possibilities that Internet offers to finish the process. For instance, the launderer

[35]FILIPKOWSKI, Wojciech. Cyber Laundering: An Analysis of Typology and Techniques. In: *International Journal of Criminal Justice Sciences* [online]. [cit. 2016-08-20]. Available from: https://www.researchgate.net/publication/222099776_Cyber_Laundering_An_Analysis_of_Typology_and_Techniques

can set up an online gambling site to mix the illicit funds with the proceeds of organized crime. Moreover, integration can be conducted by using debit/credit cards issued by offshore banks, fake loans from offshore companies or traditional purchase of real estate, online.[36]

At its simplest, cyber laundering can be described as ML through electronic money. *E-money* is an equivalent to cash in a digital form that is stored on electronic device or a server.[37] E-money is purchased from an issuing company by traditional money. The benefits of e-money, such as anonymity, safety, faster transactions or access to electronic commerce, are evident and there is no surprise that they have attracted the threat of abuse. E-money represents a real threat and its misuse can become a significant problem, especially because of these two features:

- *Inability to retrace* consists in the fact that e-money systems allow participants to deal with each other directly, without need of the assistance of financial institutions.
- *Mobility* causes that e-money can come anywhere from the world and be sent anywhere. Nowadays, e-money systems provide almost immediate transfer of money and the speed, together with the anonymity, makes difficult to trace the origin of the illegal funds.
- *Physical form,* the fact that e-money is not voluminous, is indispensably another aspect that speaks in favour of cyber laundering because it solves the problem of a bulk.[38]

It goes without saying that e-money shows a lot of promise as another effective laundering tactic. Since money launderers are very creative and current electronic payment systems provide dozens of opportunities that can be exploited, we have chosen those that show the most potential.

Pre-paid cards are an alternative to credit/debit cards. They look just like any other credit/debit cards but unlike them, they are not linked to a bank account with an overdraft. You simply cannot borrow money using pre-paid cards. Instead, you are only permitted to

[36]Ibid. (35)
[37]E-money. *www.ec.europa.eu* [online]. 2015 [cit. 2016-08-21]. Available from: http://ec.europa.eu/finance/payments/emoney/index_en.htm
[38]RICKMAN, Andy. Cyberlaundering: The Risks, the Responses. In: *Law Faculty Scholarly Articles* [online]. [cit. 2016-08-22]. Available from: http://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1326&context=law_facpub

spend the money that you or someone else has loaded onto it.[39] The evolution of pre-paid cards, from a simple gift cards to fully functioned payment instrument tied to a payment account, has brought unwanted consequences as well. Pre-paid cards can be, in the simplest possible terms, differentiated according to their scope of use and storage capacity.

Table 2: Types of pre-paid cards

Scope	**Storage capacity**
Open-Loop	Non-reloadable
Closed-Loop	Reloadable

Source: Own processing

Non-reloadable cards can be used until the balance is exhausted. They are, for instance, gift cards or mobile top-up cards what suggests their usually small denomination. The key factor here lies in the fact that there is no due diligence on the customers and this anonymity makes them a great choice for money launderers. These cards have been largely used for ML purposes in the past years. Another group of pre-paid cards create *reloadable cards.* As the name hints, they can be drawn down and topped off any time. These types of cards have a customer identification requirement, which means that the users must provide an ID. What is more, they allow cash access through ATMs and in certain cases funds transfers between users are allowed. *Open-Loop* cards are reloadable cards. These cards can be used to make purchases anywhere that are accepted. We can easily recognize them because of a credit card company's logo (Visa, MasterCard, American Express etc.). These cards allow users to transfer funds from person-to-person, withdraw money from ATMs or effect payments not only at domestic market but also at foreign one. All these features, together with the fact that their physical size makes them vulnerable to misuse by launderers that use them to make physical cross-border transportations of value, are highly desirable. *Closed-Loop* cards are usually gift cards that may only be used for purchases from a single company. Because of their anonymity, it is known that they have been used greatly by launderers, but given their low-risk, countermeasures are now more orientated to open loop cards.[40]

[39]*What is prepaid card?* [online]. [cit. 2016-08-22]. Available from: http://www.mastercard.com/hk/consumer/prepaid-card.html

[40]*Prepaid card, mobile payments and Internet-based payment services* [online]. The FATF, 2013 [cit. 2016-08-22]. Available from: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf

Money launderers are surely resourceful, so there is no surprise they try to exploit vulnerabilities in payment systems to avoid leaving financial fingerprints. As we have already introduced both types of pre-paid cards, it should be clear that non-reloadable cards have many limitations and cannot really serve for ML in a large scale. However, this does not excrete that they are not an object of interest for certain individuals. Criminals can buy gift cards and then send them to an accessory that can subsequently redeem for products, such as electronics, that can later be exchange for cash. As gift cards represent a low-risk due to the fact that they do not dispose of the access to the global ATM network, neither can be refunded, we have turned our attention to wide range of reloadable pre-paid cards that allow transactions in the payment network. Because of required due diligence and restriction on load limits that have been adopted, certain elimination of misuse was achieved. Despite that, anonymous pre-paid cards can still be obtained from the offshore jurisdictions. An example can be one company with an offshore address that provides anonymous prepaid cards. The load value is 1 000 € and the company does not require any identification. What is more, multiple cards can be ordered.[41]

In the credit card industry, many successful strategies have been developed to mitigate traditional payment frauds but we need to bear in mind that ML in this industry differs greatly from a traditional payment fraud. The difference is that payment fraud leads to a financial loss while ML does not harm financially anybody and yet has worse consequences to society at large. With that said, realizing the difference between traditional payment fraud and ML is an essential first step in development of efficient AML regimes within this industry.

Online gambling is vulnerable to a wide range of criminal activities and with electronic payments as a norm, it has evolved into a playground of money launderers. It has been identified that online gambling can serve as a mechanism to legitimize illicit proceeds of crimes. In addition, in a real world with real cash, casinos are used for ML, but this is well-known and regulated, so it is no surprise that launderers have taken it to the next virtual level. There are three principal reasons why online gambling is attractive for ML:

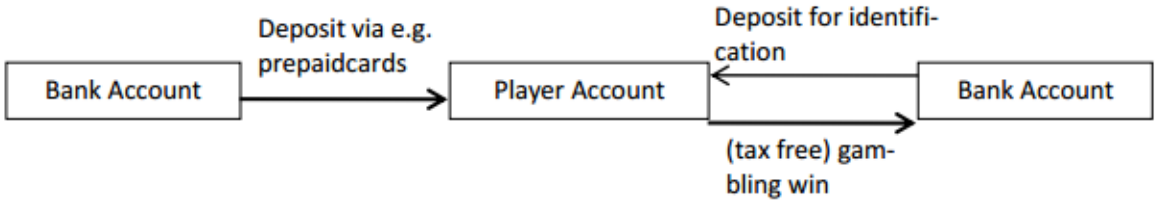
- Huge amount of transactions is one of the characteristics of online gambling and this is more than convenient for launderers.

[41]SIENKIEWICZ, Stanley. *Prepaid Cards: Vulnerable to Money Laundering?* [online]. In: . 2007, s. 22 [cit. 2016-08-23].

- Paper currency is not involved in online gambling which makes more difficult to track the flow of money.
- In many jurisdictions, proceeds from gambling are tax-free.[42]

Launderers generally use online gambling in two ways. The first option of using online gambling can be seen on picture 3 and supposes that illicit transaction occurred ex ante. The first step consists of transferring small sum of money from bank account to a player account. This phase is necessary for being able to argue that these funds were used as gambling stakes later on. This step is traceable for the financial institutions. Not traceable is the second step where launderers deposits proceeds of crime via an anonymous method, for instance via mentioned prepaid cards, to a player account. The last step is the withdrawal to the bank account as gambling win. It can be always argued that these gambling wins came from the gambling stakes deposited in the first place.

Picture 3: ML through online gambling nr.1

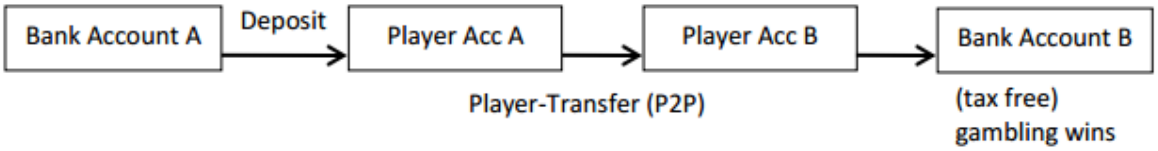


Source: www.wiso.uni-hamburg.de (19)

The second option, detailed on picture 4, considers online gambling as a payment tool. The first step is the same as in a previous case. Now, the purchaser of the illegal good deposits also his funds from a bank account to his account A. By performing a player-to-player transfer, in order to send money to the account B of the seller of the illegal goods, the seller can declare that funds are gambling win.[43]

[42]FIEDLER, Ingo. *Online Gambling as a Game Changer to Money Laundering?* [online]. In: . WiSo-Fakultät : Universität Hamburg, 2013, s. 14 [cit. 2016-08-23]. Available from: https://www.wiso.uni-hamburg.de/fileadmin/bwl/rechtderwirtschaft/institut/Ingo_Fiedler/Online_Gambling_as_a_Game_Changer_to_Money_Laundering_01.pdf
[43]Ibid. (42)

Picture 4: ML through online gambling nr.2



Source: www.wiso.uni-hamburg.de (19)

Given the above options of ML through online gambling, it is critical that operator of the online gambling site does not share information with authorities. This can be easily accomplished by using unregulated and unlicensed operations many times incorporated in offshore jurisdictions. In consideration of foregoing, this can easily affect a normal bank. These operations have bank accounts in their offshore banks that are connected via correspondent banking with other reputable banks.[44] To sum up, all types of ML in online gambling require unregulated operators as they do not have to comply with AML obligations and since illegal online gambling represents the majority of the online gambling market, it certainly is no obstacle.

Virtual games and virtual currencies are another proof that money launderers are ingenious in seizing every possible opportunity to launder their illicit funds. Virtual reality gaming is a completely unregulated means of money transfers which also creates a safe paradise for criminals including money launderers. For instance, Second life and World of Warcraft belong to a category of virtual games called Massively Multiplayer Online Role-Playing Game (MMORPGs). The user must create a virtual identity, called Avatar, to be able to operate in the virtual platform. Second life has even created its own virtual currency called Linden and this is where the problem arises. **Virtual currency** is a type of unregulated digital currency that can be traded and functions as either:

- Medium of exchange.
- Unit of account.
- Store of value.[45]

[44]Ibid. (42)
[45]Virtual currencies. *The FATF* [online]. 2015 [cit. 2016-08-25]. Available from: http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

Virtual currency, since it does not have a legal tender value in any jurisdiction, performs above functions only by agreement within the group of users. Some of the virtual currencies are *convertible*, which means they do have an equivalent value in real currency. On the other hand, *non-convertible* virtual currencies are, in the FATF taxonomy, intended to be specific to a certain domain and cannot be exchanged for real currency. The riskier type is surely that of a convertible virtual currency. This is also a case of Second life. To create such an account, the user must provide only a name and an email address, no verification is required. As we have said, to purchase virtual currency, debit/credit card or PayPal can be used what establishes some tracking but if false information was used, there is no continuation for investigative tracking. User that intends to launder money opens several accounts, providing false information. These accounts are then funded with illicit proceeds of crimes. Users can sell or purchase virtual goods and other properties by using these accounts. They may then convert virtual money into real one (for example PayPal). They can also send the virtual money to an associate in other country that consequently transfers them into real money leaving no trace of evidence.[46]

Problem of ML in the world of virtual currencies goes far beyond the virtual gaming. As we have outlined, virtual currencies are not associated solely with virtual gaming. It is a relatively new phenomenon that has emerged in the absence of regulation. The absent regulation has contributed largely to their potential benefits and the risk they pose has remained unaddressed. Virtual currencies cover a wide range of currencies from Internet, mobile coupons or airline miles to crypto-currencies. Crypto-currencies, such as Bitcoin, Litecoin, Peercoin, Dogecoin or Primecoin, are often subject to analysis whether they hold the laundering risk or not. Bitcoin "*is a pseudonymous, decentralized virtual currency system that operates purely by algorithm, using Bitcoin as the unit of currency"*[47]. The principle attributes of Bitcoin that prove essential to its survival and adverse to AML regulation, are surely the protocol's anonymity and resilience through flexibility. A simple Bitcoin transaction that involves ML happens through approximately 5 entities:

- Bitcoin sender who initiates the transaction with the dirty money.

[46]Virtual Money Laundering and Fraud. www.bankinfosecurity.com [online]. 2008 [cit. 2016-08-25]. Available from: http://www.bankinfosecurity.com/virtual-money-laundering-fraud-a-809

[47]BRYANS, Danton. Bitcoin and Money Laundering: Mining for an Effective Solution. In: *Indiana Law Journal*[online]. p. 33 [cit. 2016-08-25]. Available from: http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=11100&context=ilj

- Bitcoin receiver that accepts Bitcoins or in this example the launderer who aids the Bitcoin sender obscure the source of dirty money.
- Bitcoin miners that operate as processors and verifiers by completing blocks.
- Bitcoin team that updates the Bitcoin codebase.
- Bitcoin currency exchange that convert Bitcoins to other currencies or vice versa.[48]

In addition, Bitcoin tumblers exist. It is the technique of using a third party service to break the connection between a Bitcoin address sending coins and address they are sent to. In other words, tumblers are used to mix one's funds with other people's money, intending to obscure the trail back to the funds' original source.[49] In traditional financial systems, the equivalent would be transferring funds through banks located in jurisdictions with strict bank secrecy. This analogy certainly makes sense, mainly because it has similar features to smurfing of deposits, where large amount of cash is split up and integrated into the financial system. What is more, ML is being more and more associated with Bitcoin online casinos. The launderer can simply play with dirty coins and then withdraw them receiving Bitcoins that have been transferred several times. Laundering Bitcoin works and using Bitcoin casinos is only one of many ways to legitimize illicit proceeds.[50]

2.2 Potential of cyber laundering

Even if cyber laundering is still in its infancy, it is without doubt a growth industry whose potential is extensive. It constantly evolves and presents itself with unforeseen opportunities that make it particularly difficult for regulatory authorities to respond. In this subchapter, we have pursued to evaluate potential of cyber laundering by briefly analysing the growth of Internet that is a main trigger of the whole cyber-issue and ultimately potential of cyber-laundering methods mentioned in previous subchapter.

[48]Ibid. (46)
[49]A simple guide to safely and effectively tumbling bitcoins. *www.darknetmarkets.org* [online]. 2015;; [cit. 2016-08-30]. Available from: https://darknetmarkets.org/a-simple-guide-to-safely-and-effectively-mixing-bitcoins
[50] Using Bitcoin Casinos To Launder Bitcoin. *www.bitcoinbabeau.wordpress.com* [online]. 2016 [cit. 2016-08-30]. Available from: https://bitcoinbabeau.wordpress.com/2016/04/13/using-bitcoin-casinos-to-launder-bitcoin/

Potential of Internet

There is no doubt that cyber laundering is one of the undesirable outcomes of globalization of the Internet. Without features it offers, there would be no cyber laundering as it creates conditions necessary for its formation and further evolution. The access to the Internet has become a common luxury. Nowadays, almost 50 % of population has access to the Internet in comparison with only 1 % in 1995. Internet is indispensable for a number of activities and its growth does not have steady trend, on the contrary. The table below demonstrates that there are nearly 4 billion of Internet users and the growth between years 2000 and 2016 has reached 900 %.

Table 3: World Internet usage

World Internet usage and population statistics - June 30, 2016					
World region	**Population 2016**	**Internet users 30 June, 2016**	**Penetration (% of popl.)**	**Growth 2000-2016**	**Users % of table**
Africa	1 185 529 578	339 283 342	28,6 %	7 415,6 %	9,4 %
Asia	4 052 652 889	1 792 163 654	44,2 %	1 467,9 %	49,6 %
Europe	832 073 224	614 979 903	73,9 %	485,2 %	17,0 %
Latin America	626 054 392	384 751 302	61,5 %	2 029,4 %	10,7 %
Middle East	246 700 900	132 589 765	53,7 %	3 936,4 %	3,7 %
North America	359 492 293	320 067 193	89,0 %	196,1 %	8,9 %
Australia	37 590 704	27 540 654	73,3 %	261,4 %	0,8 %
World Total	**7 340 093 980**	**3 611 375 813**	**49,2 %**	**900,4 %**	**100 %**

Source: Internet world stats (33)

This, certainly is a staggering success of the new era that has brought possibility of unlimited communications, abundant resources and information. In consideration of the foregoing, there are many threats that have been born with the advent of the Internet such as addictions, viruses, phishing and other cybercrimes among which cyber laundering undoubtedly belongs. The United Nations at the “Human Rights Council” in June 2016 declared that disconnecting people from the access to the Internet is a violation of human rights and that access to the Internet is a basic human right. A majority approved the non-binding resolution but there were some defendants. For many, it is not surprising that the authoritarian regimes of Russia, China and Saudi Arabia opposed the proposal as they have vague stance on human

rights in general.[51] Number of countries, including France, Finland, Estonia, Spain, Greece, Costa Rica has already made access to the Internet a basic human right and after this non-binding resolution that has been supported by more than 70 countries, there is a good chance that also other states will follow this path.

At the beginning of this chapter, we have outlined that Internet aids cyber laundering for its irreplaceable features and because it has become a common luxury accessible for many. The above text has tended to draw attention to the fact that era of Internet is experiencing remarkable progress what might adversely influence the evolution of cyber laundering.

Potential of online gambling

As the Internet access is growing at an exponential rate, aforementioned online casinos are becoming a safe haven for money launderers. We have dedicated some time to clarifying why online gambling is convenient option for ML. As the table 4 shows, significant growth was recorded in the quantity of new licensed online gambling sites between years 2009 and 2013.

Table 4: Number of online gambling sites in certain jurisdictions

Number of online gambling sites				
Jurisdictions	**May 2009**	**July 2010**	**January 2011**	**November 2013**
Alderney	66	96	98	120
Cyprus	32	45	47	120
Gibraltar	216	255	262	312
Isle of Man	15	26	38	79
Netherland Antilles	271	312	280	456

Source: Banks, J. (1)

However, licensed casinos are only a fraction of a number of unlicensed casinos that are created every day. The growing trend of licensed online gambling sites can only serve as an indicator how big potential this business has. The estimations from 2006 show that beyond

[51]Internet Access Is Now A Basic Human Right. *www.gizmodo.com* [online]. 2016 [cit. 2016-08-25]. Available from: http://gizmodo.com/Internet-access-is-now-a-basic-human-right-1783081865

the 2 347 licensed online casinos, there are further 12 476 unlicensed sites.[52] Given the year of this estimation, it is expectable that there are many more at present.

The main aspects that differentiate licensed online casinos from unlicensed ones are:

- Licensed casinos usually comply with AML policies.
- Certain regulatory authorities audit them.
- They may require the deposit of funds over the institutions that are subject to AML regime.[53]

Still many states are yet to develop legislation that responds effectively to online gambling but there are jurisdictions that have adopted a wide range of responses to online casinos. The responses vary with states that prohibited all forms of Internet gambling on one side, and countries that placed some restrictions by making legal only certain forms of gambling on the other. Guarantee, that online gambling is transparent, is goal of most of the regulatory models and this is being achieved by monitoring transactions, certification of gambling technologies, licensing or taxation. Although there are many jurisdictions that have already introduced legislation related to the misuse of online gambling for ML purposes, there is one significant problem that remains: there are many companies situated outside of the borders that offer products available to other citizens, which vastly amplify the problem. However, any kind of estimation of the black market is challenging, it has been estimated that less than 15 % of the 14 823 online casinos that are available by EU citizens hold any kind of license.[54]

The below table 5 demonstrates the selection of countries where online gambling is not regulated at all, which means that players from these countries are accepted in numerous foreign online casinos unrestrictedly.

[52]Computer Emergency Response Team - Laboratoire d'Expertise en Sécurité Informatique (2006). Online Gaming Cybercrime: CERT-LEXSI'S White Paper, July 2006.
[53]Jackpot! Money laundering through online gambling. *www.mcafee.com* [online]. 2014 [cit. 2016-08-25]. Available from: http://www.mcafee.com/es/resources/white-papers/wp-jackpot-money-laundering-gambling.pdf
[54]BANKS, James. *Online gambling and crime: causes, controls and controversies*. Farnham: Ashgate, 2014. ISBN 978-1-4724-1449-6.

Table 5: Regulatory status of online gambling in selected jurisdictions

Country	Online Casino gambling	Online Bingo	Online Lottery	Online Sports betting
Andorra	not regulated	not regulated	not regulated	not regulated
Faroe Islands	not regulated	not regulated	not regulated	not regulated
Kosovo	not regulated	not regulated	not regulated	not regulated
Lichtenstein	not regulated	not regulated	not regulated	not regulated
Macedonia	not regulated	not regulated	not regulated	not regulated
Monaco	not regulated	not regulated	not regulated	not regulated
Moldova	not regulated	not regulated	not regulated	not regulated

Source: www.simonsblogpark.com (60)

As we have previously stated, ML through online gambling requires non-regulated sites where operators are not obligated to share information with authorities. That might indicate that we must draw our attention to jurisdictions where casinos are poorly regulated or non-regulated at all. But, an illegally operating online casino can be hosted anywhere, we should not make any connection between online gambling being not regulated in a country and the number of online casinos operating without a license in said country.

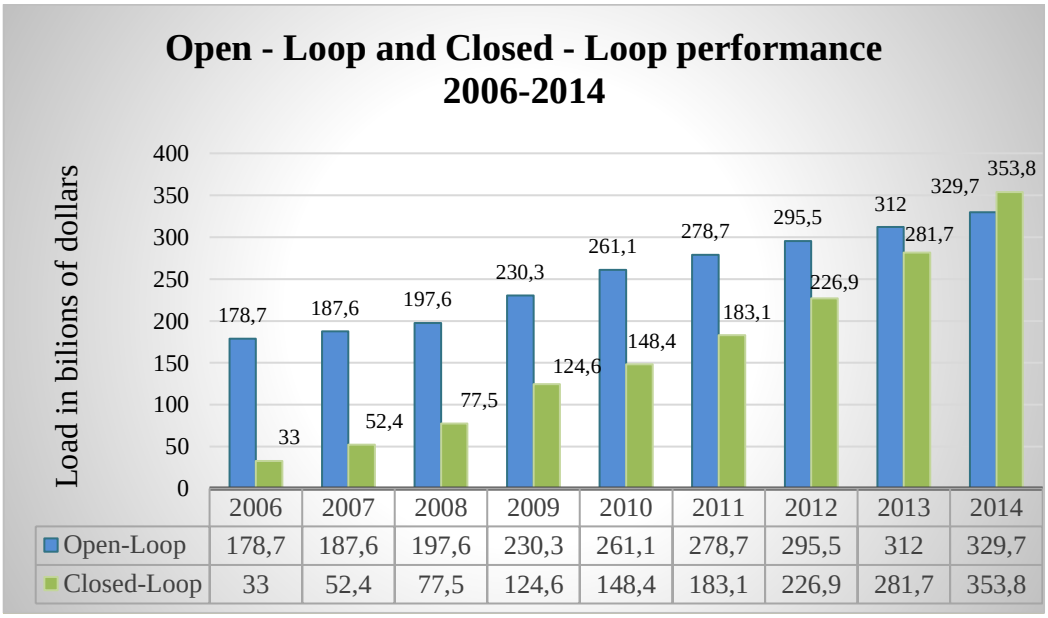
Moreover, the problem also occurs when casinos are only regulated as entrainment operations rather than financial, but as we already know, casinos offer many financial services (accounts, cash issuing, foreign exchange) so this problem has logical justification. To improve the situation in this sector and not to increase potential of this ML source, casinos should pay attention to customer's behaviour and be able to recognize what is abnormal. With that being said, it is not casino's responsibility to determine whether they are dealing with ML or not. Their role is to identify and report and it is then up to law enforcement and other responsible authorities to decide if ML is taking place or not.

Potential of pre-paid cards

Potential of pre-paid cards in cyber laundering cannot be underestimated. Referring to our previous point that anonymity of non-reloadable pre-paid cards surely is one of the factors that excite launderer's attention, the new emerging attacks interestingly involve reloadable cards. This type of card undoubtedly possesses qualities, which are convenient for

launderers. Put differently, the current status of credit card industry within ML scope could be described as evolving rather than growing. Card management platforms, the platforms that are being run by financial institutions that issue these cards, hold potential for ML. When hackers happen to get into these platforms, they steal card numbers and change credit balances. As long as these credit balances are changed, for instance from 5 000 to 10 000 €, they simply remove spending limits. Consequently, the cash is then laundered by buying cars or any other valuable assets. As the text indicates, these emerging attacks are insider ones and exploit the good knowledge of these platforms. To mitigate these insider misuses of card management, everything comes down to the level of security.[55] Potential threat of pre-paid cards in the world of ML should be also seen in the context that it is a popular and fast growing product. Graph 1 shows that the pre-paid market continues to have a strong growth in both of its segments.

Graph 1: Open - Loop and Closed - Loop performance



	2006	2007	2008	2009	2010	2011	2012	2013	2014
Open-Loop	178,7	187,6	197,6	230,3	261,1	278,7	295,5	312	329,7
Closed-Loop	33	52,4	77,5	124,6	148,4	183,1	226,9	281,7	353,8

Source: Mercator Advisor Group (67)

Both segments have recorded gradual increase in the past years and with the current electronic age, there is no reason to expect the opposite trend for the future. There are dozens of competitors in the market place that launch their products meeting the demand of the

[55]How to Fight Prepaid Card Fraud. *www.bankinfosecurity.com* [online]. 2014 [cit. 2016-08-26]. Available from: http://www.bankinfosecurity.com/interviews/how-to-mitigate-prepaid-card-fraud-i-2149

market and responding to their competitors. The question remains whether with this rapid development, the full risk assessment at the product level is done.

Potential of virtual currencies

There are hundreds of virtual currencies, some of them being riskier than others. They entail risks as eventual vehicles for ML because of not only their nature and benefits but mostly the development of effective AML regimes is at early stage within this segment. Beyond question, it is not an easy task to regulate them, as they are not entirely transparent and operate on global scale. To demonstrate that virtual currencies have a great potential, we have summarized characteristics that confirm this assumption:

- **Scarcity of transparency**.
- **Global scale preformation** that includes also non-cooperative countries increases their potential AML/CTF risks. The fact that Internet is a basic building block for their development further raises concerns about their future potential and inability to control it. Anonymity that Internet offers is what allows them to be ahead and outgo regulation.
- **Convertibility** is a critical feature without which they would not have such a power. Anonymising software, through which the transition from virtual to real currency is executed, aids to escape from the regulatory eyes and finish the act of ML.
- **Unregulated subjects,** such as individuals or private companies, are often producers of virtual currencies.

Otherwise stated, they add another layer of complexity because, unlike traditional currency transfer, there is no physical material to observe or intercept for proof of illegal activities. In the previous subchapter, we have offered very simple laundering transaction using Bitcoin. The possibility to exchange Bitcoins for other currencies and to transfer through an endless number of diverse Bitcoins addresses for puzzlement frustrates any AML efforts. With this being said, according to Robinson, Bitcoin is not a great way to launder money, on the contrary, it is a great way to collect terrorist funds because it is entirely opaque.[56]

[56]Bitcoin tumbler: The business of covering tracks in the world of cryptocurrency laundering. *www.ibtimes.co.uk* [online]. 2015 [cit. 2016-08-30]. Available from: http://www.ibtimes.co.uk/bitcoin-tumbler-business-covering-tracks-world-cryptocurrency-laundering-1487480

With respect to aforementioned, International Monetary Fund (IMF) holds the view that virtual currencies do not poses systematic risks so far mainly due to the limited linkage to financial system, limited market values and transaction volumes.[57] Fortunately, EC has adopted a new Directive proposal in July 2016 that proposes extension of AML regulation to both virtual currencies and custodial wallet providers. It will be clearer soon how this amendment contributes to the ML prevention.

Everything above-said indicates the gravity of the issue and demonstrates that potential of cyber laundering can be bigger than expected. We suppose that cyber laundering certainly is an increasing function of the Internet accessibility and its unlimited possibilities. Without effective regulation, the great potential that access to the Internet brings will also create the further evolution of the cyber laundering. The question of regulation in terms of cyber laundering is principal but also very vulnerable. Evaluating potential of cyber laundering is threatening and predictions do not oppose it. We are not exaggerating when we say that after the world is globally connected and e-money becomes a norm, ML begins to be undetectable and unpreventable.

[57]HE, Dong a Karl HABERMEIER. Virtual Currencies and Beyond: Initial Considerations. In: *IMF* [online]. s. 42 [cit. 2016-08-29]. Available from: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf

3 Terrorist financing

In recent years, terrorism has become very dangerous throughout the world. The amount of terrorist attacks has been increasing and it seems that there is not much we can do to slow it down. It is matter of fact that terrorism has become a part of our daily lives and that we are living in times when impact that living with terrorism has on individual lives is undoubted. Financing of terrorist attacks started to be associated with ML after the terrorist attack of World Trade Centre on 11 September 2001.

Defining terrorism itself is not an easy task because it might have considerable political, religious and national implications from country to country. Terrorism can be interpreted as the unlawful use of violent acts to evoke fear, especially against civilians, usually for political, religious, or ideological purposes.[58] The aim of intimidating population differentiates financing of terrorism from other crimes where financial gain is of prime importance.

One can ask what terrorism has to do with ML. This question is reasonable because there are obvious differences and although similarities between ML and terrorism are undeniable, they are not evident at first glance. The objective of this chapter is to demonstrate the existence of these similarities and to explain that dealing with ML requires considering terrorism and the mechanisms used to finance it as well.

Terrorist financing (TF) is a special term that has come to represent both, the collection of funds for terrorism and the movement of these funds to terrorist groups that consequently enable them to perform acts of terrorism. Let us mention another generally accepted definition used by authorities. The World Bank defines TF as "*financial support, in any form, of terrorism or of those who encourage, plan or engage in it.*"[59] This rather broad definition begs the question of what do we know about TF?

[58]Terrorism. *www.en.oxforddictionaries.com* [online]. 2014 [cit. 2016-08-26]. Available from: http://www.oxforddictionaries.com/definition/english/terrorism

[59]SCHOTT, Paul. *Reference guide to Anti-Money laundering and combating the financing of terrorism*. [e-book] .2nd ed. Washington, D.C.: World Bank, c2006. ISBN 0-8213-6513-4. Available from: https://books.google.cz/books/about/Reference_Guide_to_Anti_money_Laundering.html?id=qRJlAXxAOCwC&redir_esc=y

3.1 Sources of Terrorist financing

In this section, we have pursued to answer the question posed in previous subchapter and that is what we know about financing of terrorism. Before that, we have considered beneficial to begin with clarification of TF's requirements that establish the need for these sources. The process of detection and identification of TF requires understanding the funding requirements of a terrorist group. What do we mean by funding requirements? Not only do we mean costs related to conducting acts of violence but also funds needed for development of such a terrorist organization.

As we have made short introduction regarding the funds of a terrorist organization, we are now able to summarize that TF requirements can be divided into two general areas:

- Funds necessary to cover specific terrorist operations, including directs costs associated with terrorist attacks.
- General costs to develop and maintain infrastructure of such an organization and to promote the ideology necessary for retaining and acquiring members.[60]

Even though total funds needed are large, the direct costs of a terrorist attack may be very low. The table 6 illustrates the direct costs of some terrorist acts that happened recently and in the past years. It is alarming that these costs are relatively low and negligible in comparison with billions of euros that combating terrorism requests.

Table 6: Estimated cost of selected terrorist attacks

Attack	**Date**	**Estimated costs in €**
Paris Bataclan shooting	13.11.2015	9 350
Paris Charlie Hebdo shooting	07.01.2015	5 000
London transport system	07.07.2005	10 000
Madrid train bombing	11.03.2004	9 000

Source: RYDER, N. (4)

How is the above fact about direct costs related to the fight against ML/TF? Before we explain it, it is extremely important to realize that transforming huge amount of money is

[60] Terrorist financing. *www.fatf-gafi.org* [online]. 2008 [cit. 2016-08-26]. Available from: http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf

one of the leading indicators for banks that arouse suspicion. On that account, it is obvious that detecting the transfer of such a small number of funds, before act of terrorism has occurred, is challenging, if not impossible. This significantly affects not only a misuse of financial systems for illicit activities but it also eases the realization of terrorism. All the same, nowadays, it is of prime importance for authorities and financial institutions to track the flow of illicit funds, as it impedes the operation of terrorists and helps track them down. We put a sufficient emphasis on understanding of TF's requirements, which was beneficial for our next move towards clarification of sources of TF. It goes without saying that terrorism costs money. Without them, any kind of a terrorist organization would not be able to operate and conduct its acts of violence. There are certain attributes that a terrorist organization takes into account before creating a portfolio including quantity, legitimacy, security, reliability, control and simplicity.[61] Each of these attributes has its own benefits and drawbacks and there is no perfect source. For this reason, it is critical to create a well-diversified portfolio from available sources that can be divided into four main categories:

- Illegal activities.
- State sponsorship.
- Legitimate activities.
- Popular support.

Illegal activities are believed to go hand in hand with terrorism. We cannot negate it but as we see later on, it is not a rule. The most typical illegal activities involve smuggling, kidnapping, pirating and extortion but also some more "sophisticated" mechanisms such as revolutionary taxes. Illegal activities remain advantageous and terrorists certainly do not lack skills needed to undertake such crimes. The most crucial is that it guarantees them to maintain control since they do not have to entirely rely on other sources of funding. It allows them to be independent and more powerful. The main disadvantage that comes with illegal acts is that some types of these activities may cause public-relationship disaster especially when they antagonize population by committing too many kidnappings, extortions and so on.

[61]FREEMAN, Michael. The sources of terrorist financing: theory and typology. In: *Calhoun: The NPS Institutional Archive* [online]. 2011 [cit. 2016-08-30]. Available from: http://calhoun.nps.edu/bitstream/handle/10945/47781/Freeman-The-Sources-of-Terrorist-Financing_2010.pdf?sequence=1

State sponsorship, although it was one of the principal sources, has declined rapidly in the past years. This decrease can be certainly assigned to a great amount of work that regulatory authorities have done in this matter. For terrorists, the state sponsorship can be convenient considering the fact that it can provide a large quantity of funds and the simplicity by which they get them is irreplaceable among other methods. Disadvantages that state sponsorship can bring are numerous. One of them is control. It is a simple logic that state can utilize its support to control activities of terrorists and to force them to act in its favour. This may very easily result in a situation when terrorist may be forced to undertake acts that they would not otherwise commit. Another disadvantage that comes from state ownership is that state, with its tactics and policies, can change. This is an actual one because many states have stopped funding terrorism in regard to international pressure.[62]

Legitimate sources can also generate a great amount of funding for a terrorist organization. The general public may not realize that terrorists often operate legal entities to generate funds for their activities. This denies the general misperception that TF comes only from criminal activities. Al Qaeda, for instance, ran many legal businesses in Sudan including farms, trading companies, a tannery, a bakery and so on.[63] There are many more examples that could be demonstrated to show that a proportion of legal financing is huge. Why is it so? The answer to this question is security. For TF, the question of security is ultimate, as there is little that can be done to target such activities. In addition, criminal activity always attracts attention that may have fatal consequences for a terrorist group itself. Also, legal activity may draw unwanted attention. The legal financing can be very hazardous as it may provide authorities with a great insight into the terrorist cell. Whereas legal business is obligated to keep records and can be audited, it can supply authorities with key information about terrorist groups. Legitimate financing also brings another obstacle that should be under consideration of terrorists. In today's competitive market, it is not easy to make a profit. The question is: Are terrorist educated enough to be able to outperform all the other businesses in the marketplace? If the question is negative, they will surely become more attracted to illicit activities.

[62]Ibid. (61)
[63]BURKE, Jason. *Al-Qaeda: the true story of radical Islam*. 3rd ed. London: Penguin, 2007. ISBN 9780141031361.

Popular support is also one of the options. The support that comes from sympathetic population can yield large portion of the revenue. It must be recognized that also charitable donations generate funds for radicals. For instance, the Global Relief Foundation and the Al-Wafa organization were associated with Al Qaeda. This not only causes a serious problem in terms of financing terrorism but it can also be an alarming signal of their legitimacy. [64]

According to the aforementioned, we can conclude that there is no ideal source of financing as each source has its benefits and drawbacks across the mentioned attributes. Well-created portfolio can minimise the threat of losing one principle source and enable to operate through the bad times.

3.2 The link between Money laundering and Terrorist financing

To understand the nexus between TF and ML, it is essential to realize that some funds raised to finance such activities must be laundered. Hence, AML processes in financial institutions are vital for identifying and tracking of TF as well.

The linkage between these two terms arises also from the fact that terrorists use techniques like those of money launderers to evade attention of authorities and to protect identity of their sponsors. Irrespective of the fact that TF may also originate from legitimate sources, it is also inevitable to conceal the source. Why is it fundamental? If individuals are successful in disguising the origin of their financing, the financing activity can continue, as it remains undetected. This also implies that the mechanisms used for ML are basically the same as those for concealing the source of, and uses for, TF.[65] In this respect, criminal assets and terrorist assets pose the same menace to financial systems and that being so, the actions designed to combat money launderers when they channel their proceeds through financial systems may also apply with the same success in fighting TF. In addition, distinction is

[64]Ibid. (61)
[65]Ibid. (61)

useless, however, since the intention of public policies is not to address the issue of the processing of illicit funds, but the funds themselves and the organizations behind them."[66] Introduction of this subchapter stated that connection between ML and TF clearly exists and that it would be incomplete to discuss concept of ML without mentioning TF. That being said, there is a considerable difference between them that should be stated. As we have outlined earlier, monitoring of financial transactions in traditional ML is done to link the illicit funds to a criminal act that has taken place already. Investigation related to TF is carried out to prevent certain individuals from gaining access to proceeds of crime that could likely finance future terrorist activities. In a nutshell, it is done to foil a crime from happening.[67] Moreover, it is worth repeating that laundering of criminal proceeds leads to giving a legal appearance to dirty money while laundering of terrorist funds attempts to obscure the link to their funding sources.

Realization that ML and TF has many features in common and that these mechanisms are in certain cases undoubtedly related to one another, has led to the fact that almost all regulatory authorities or jurisdictions incorporated Counter-Terrorist Financing (CTF) measures, as part of their requirements or within their legal systems.

[66]THONY, Jean-François. In: *IMF* [online]. [cit. 2016-08-30]. Available from: http://www.imf.org/external/np/leg/sem/2002/cdmfl/eng/thony.pdfttp://www.imf.org/external/np/leg/sem/2002/cdmfl/eng/thony.pdf

[67]Terrorist financing: definition and methods. *www.fidis.net* [online]. [cit. 2016-08-30]. Available from: http://www.fidis.net/resources/fidis-deliverables/identity-of-identity/int-d2200/doc/27/

4 Combating Money laundering and Terrorist financing on international level

AML regulation started at multinational level in late 80s, principally due to the unsuccessful US war on drugs and culminated in 1989 when the FATF was established. Since ML has vast objectionable consequences, impeding the social, economic, political, and other development of societies worldwide, we have recently witnessed far-reaching changes in the penal law systems of all developed countries. Furthermore, most countries have taken necessary measures not to end up on the "blacklist" of the non-cooperative countries disclosed regularly by certain authorities.

No one can argue that implications of increasing globalization are as positive as negative. The fact that globalization has been accompanied by the growth of illegal activities that have boosted demand for ML is one of those adverse ones. ML and TF certainly are global menaces, primarily because they both can exploit any jurisdiction, and therefore it is fundamental to have effective AML/CTF mechanisms in place. Since no country is immune and these activities occur in both developed and yet developing countries, their successful implementation can considerably mitigate the adverse effects they bring.

The chapter dealing with AML/CTF procedures is an essential part of this diploma thesis and necessity needed for its successful accomplishment. For that reason, we put considerable amount of time to approach authorities dealing with AML/CTF measures in the most logic way. Within this important chapter, we have pursued to present the most influential governmental and non-governmental agencies together with briefly mentioning the role of sanctions within AML/CTF.

4.1 The Financial Action Task Force[68]

The FATF is an acronym for the Financial Action Task Force, which is an inter-governmental body established in 1989 on the initiative of the G7 in Paris. It currently comprises 35 member jurisdictions that are supposed to be the biggest financial centres. Its aim is to create policies to combat ML and in 2001, with an increased numbers of terrorist

[68] *FATF* [online]. [cit. 2016-09-01]. Available from: http://www.fatf-gafi.org

attacks, the purpose expanded to act on TF.[69] Thus, the FATF can be defined as a policy-making institution and its main objective is to set standards and to introduce effective measures for combating ML/TF and other potential threats that can endanger financial systems. It is important to note that the institute of the FATF is not legally enforceable on national authorities but given its strong position and inevitable role it plays in setting and consequently auditing a national authority's compliance with AML laws, it is recommended to comply with it.

The FATF monitors the countries' progress in implementation of requisite measures. Furthermore, it regularly reviews ML/TF techniques that are being continuously evolved and subsequently adjusts countermeasures, responding to these changes. In addition to all forgoing, in collaboration with other international authorities, the FATF attempts to identify vulnerabilities at national levels aiming at protecting the legitimate financial system from abuse. Since no country is immune to being misused for illegal purposes, all countries should implement the framework of measures produced by the FATF to efficiently fight ML/TF. In spite of the fact that countries' legal and operational frameworks differ and that financial systems can also vary, countries should implement these international standards and adapt them to their specific needs.

In 1990, the FATF originally proposed **40 recommendations** against ML. These recommendations are mandates for action by country if the country wants to be considered as meeting international principles. The first revision of recommendations in 1996 was necessary, whereas ML methods have changed and become more sophisticated in response to countermeasures but principally it was essential to broaden the scope well beyond drug-ML. Given the expanded mandate dealing with issue of TF in 2001, the FATF created the eight (later ninth) special recommendation on TF. There were a number of revisions in previous years that have been endorsed by more than 180 countries and are now recognized as international standards. For these revisions is typical that they try to reflect new and emerging threats and reinforce many of existing recommendations. These recommendations are included under the certain sections that can be found in Appendix.

[69]In 2008 the FATF mandate was expanded again to include financing of proliferation of weapons of mass destruction as well.

It is critical that all jurisdictions apply these international standards to maximum extent and cooperate with one another. Consequently, the FATF monitors implementation of these standards and what is more, discloses jurisdictions with strategic deficiencies. There is logic behind this approach. Identified countries with certain weaknesses are brought to the attention so other jurisdictions can apply risk-sensitive approach when dealing with them. In this regard, between the years of 2000-2006, the FATF carried out process on non-cooperative countries and territories (NCCTs). Since 2007, International cooperation review group (ICRG) has replaced the NCCTs process. The ICRG also analysis high-risk jurisdictions and suggests actions leading to risk mitigation. The purpose of the review process is to determine most threating AML/CTF weaknesses and to develop an action plan to address them. The action plan also requires a high-level political commitment that is inevitable for implementation of legal and regulatory reforms.

Once the action plan has been established, the FATF arranges a visit to ensure that implementation of the legal, regulatory and institutional reforms is on-going and if there is a political commitment necessary for improving the AML/CTF regime. A positive outcome then leads to a consideration of removing the country from public identification. This idea will be developed in more detail in chapter 6.

4.2 Anti-money laundering Directives in European Union

As ML constantly evolves towards new sophisticated techniques, so the legislation reconsiders its attitude and attempts to respond to it in the most effective manner. As it was briefly mentioned in the first chapter, the EU is the primary driver of AML legislation in Europe. Up until now, there have been four Directives that are designed to protect the financial system from misuse and to shield some of the vulnerable professions. Furthermore, the Single Market has provided increased possibilities for launderers so the Directives were necessary to protect the goals of EU too.

The first Directive - The Council Directive of 10 June 1991 on the prevention of the use of the financial system for the purposes of ML (91/308/EEC).

Enhancement of ML and the need to defend the promising goals of newly created EU led to the creation of the first EU AML Directive in 1991. As the name of the Directive indicates, its concern was mainly jeopardizing the financial systems. In these times, the financial system went through a significant change, so the concerns that it could lead to an abuse were in place. It can be said that the first Directive created an initial framework for the consequent Directives. It focused on the laundering of money derived from drug related crime through the banks and, as such, obligated banks and other regulated firms to maintain systems for customer identification, staff training, record keeping and suspicious transaction reporting. However, the Directive did fail to extend the provisions of the Directive and fight this growing menace.[70]

The second Directive - Directive 2001/97/EC of the European Parliament and of the Council of the European Union of 4 December 2001.

The goal of the second Directive was to improve the existing provisions established by the first Directive and to fill the gaps in the legislation highlighted by the FATF 40 recommendations. The Directive expanded the definition of ML, considering also underlying offences such as corruption. Moreover, the Directive made clear that also currency exchange offices and money transmitters were part of the Directive as they also were vulnerable to ML procedures. Furthermore, the second Directive also added the authority to identify, trace, freeze, seize and confiscate any proceeds related to criminal activities.[71]

The third Directive- Commission Directive 2006/70/EC of 1 August 2006.

It was the third Directive in field and the first that covered TF. The third Directive considered the revision of the FATF's AML/CTF standards of 2003. The first and second Directive were not successful to cover all areas where preventive measures where needed to be applied. Thus**,** the third Directive was the result of the realization of the vulnerability of designated non-financial businesses and professions to the furtherance of ML transactions. In other

[70]History of the European Union Anti-Money Laundering and Financing of Terrorism Directives. *www.Anti-Moneylaundering.org* [online]. 2015 [cit. 2016-09-02]. Available from: http://www.Anti-Moneylaundering.org/Europe.aspx

[71]Ibid. (70)

words, the Directive was applicable to lawyers, notaries, accountants, real estate agents, casinos, encompassing trust, and company services, exceeding 15 000 €.[72]

The fourth Directive - Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of ML or TF.

Its aim is to remove any ambiguities in the former Directive and refine consistency of AML/CTF measures across all Member States. As usually, it took into consideration the current revised recommendations of the FATF from 2012. The fourth Directive has extended the scope of regulation to include:

- The establishment of central registers of Ultimate Beneficial Owners (Central UBOs-register).
- Threshold for cash payments has been lowered from 15 000 to 10 000 €.
- More caution with Politically Exposed Persons (PEPs).[73]
- Expanded to include the whole gambling sector, not only casinos.[74]

The first point certainly deserves a few words. For several years, criminals in Europe have misused the anonymity of offshore companies and accounts to conceal their financial dealings. The Directive states that EU members are obligated to establish a central UBOs-register. It is believed that its establishment will help lift the veil of secrecy of offshore accounts and recognizably aid the fight against ML. The fourth Directive defines a UBO as:

- Any natural person who ultimately owns or controls the customer.
- The natural person on whose behalf a transaction or certain activity is being undertaken.
- Considering the corporate entities, the natural person who ultimately holds a shareholding, controlling interest or ownership interest over 25 % of the shares/voting rights.

[72]The third EU directive on money Laundering and terrorist Financing. In: VYHNÁLIK, Ján. *NBS* [online]. ť [cit. 2016-09-02]. Available from: http://www.nbs.sk/_img/Documents/BIATEC/BIA09_05/11_15.pdf The third EU directive on money Laundering and terrorist Financing

[73]A **PEP** is someone who has been entrusted with a prominent public function. A PEP presents an increased risk for potential involvement in bribery or corruption by virtue of their position and therefore represent also enhanced risk in terms of ML/TF.

[74]The Fourth EU Anti Money Laundering Directive. *www2.deloitte.com* [online]. [cit. 2016-09-02]. Available from: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/investmentmanagement/ie_2015_The_Fourth_EU_Anti_Money_Laundering_Directive_Deloitte_Ireland.pdf

The following information should be at least included in the UBO- registers: name, month and year of birth, nationality, country of residence and nature and extent of the beneficial interest held. In respect of trust, the trust register should incorporate at least the identity of the settlor, trustees, protectors, beneficiaries or class of beneficiaries and any other natural person that exercises effective control over the trust.[75] This step finally breaks the long tradition of hidden company ownership and curtails the ability to use anonymous shell companies for concealing illegal activities.

In addition to forgoing, the new Directive is supposed to better accommodate the EU's AML regime with the US's, mainly by accepting more risk-based approach compared to the precedent Directives. This will surely be welcoming amendment for entities operating in both jurisdictions.[76]

Furthermore, on 5 July 2016, as a response to growing threat of terrorism, the European Commission (EC) has approved number of important amendments to the Directive. Amongst the most important are mentioned virtual currencies that have finally been brought under the scope of the Directive. Another important amendment that is worth mentioning concerns prepaid cards. The EC has lowered thresholds for identification and widen customer verification requirements from 250 to 150 € and removed its exemption in respect of online use of prepaid cards.[77]

4.3 Sanctions

Sanctions are imposed for variety of purposes, including pressurising a particular jurisdiction or regime to change its behaviour, or to prevent TF. Many different sanctions exist, such as

[75]EU Directive 2015/849 of the European parliament and of the council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849, § 6ab

[76]AML global alignment: Two steps forward, one step back. *www.pwc.com* [online]. 2015 [cit. 2016-09-02]. Available from: http://www.pwc.com/us/en/financial-services/regulatory-services/publications/assets/aml-global-alignment.pdf

[77]The Fourth EU Anti Money Laundering Directive European Commission Update. *www2.deloitte.com* [online]. 2016 [cit. 2016-09-02]. Available from: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/IE_2016_fourth_EU_AML_Directive.pdf

travel bans, asset freezes, trade embargoes and other restrictive measures. Restrictions may target governments of third countries, or non-state entities and individuals.

Relevant for us is that these sanctions are understood also as *another element of the AML/CTF framework* that surely contributes to combating ML/TF. Even though compliance with AML obligations does not totally equal compliance with financial sanctions obligations, the key similarities are the use of judgement and the adoption of a risk-based approach. Moreover, as it will be seen in chapter 6, AML/CTF due diligence products includes also compulsory sanctions screening. As it is evident, AML/CTF framework and imposed sanctions are closely linked to each other and complement each other.

Sanctions have many forms, but the most relevant types are:

- *Financial sanctions*, which are directives issued by governments, the EU or the United Nations (UN), prohibiting or restricting the provision of financial services to certain countries, regions, individuals and entities.
- *Trade sanctions*, which are intended to prevent trade in particular commodities or services into and/or out of particular jurisdiction.[78]

Taking into consideration the increasing level of legalisation of the international system that concerns wide range of issues from international terrorism to ML, restrictive measures are used not only for policy-sensitive issues of crisis management but also for the fight against organized crime and cyber security. Within this subchapter, the most relevant and powerful sanctions have been briefly mentioned.

4.3.1 European Union and United Nations sanctions

The UN Security Council decides and administers the sanctions regimes, which are binding on UN Member States. This means that UN Member States are legally obliged to implement these sanctions. While its approach is certainly laudable form a humanitarian perspective, it has increased the complexity for firms that need to implement them.[79]

[78]There are also diplomatic or travel restrictions. In addition, sectoral sanctions are an entirely new breed of sanctions.
[79]Sanctions. *www.un.org* [online]. 2016 [cit. 2016-09-01]. Available from: https://www.un.org/sc/suborg/en/sanctions/information

In Europe, the *EU* promulgates and administers financial and trade sanctions as non-legislative acts, which means they have direct effect for all EU Member States. These restrictive measures are a crucial tool of the EU's Common Foreign and Security Policy with an important reach in the field of ML/TF. They are normally wider than those imposed by the UN Security Council.[80]

Individual countries also promulgate and administer their own sanctions. The great example can be US that administers and enforce financial and trade sanctions in the US but as we will see in the next subchapter, it has extraterritorial effect.

4.3.2 The Office of Foreign Assets Control

The Office of Foreign Assets Control of the US Department of the Treasury (OFAC) is a financial intelligence that administers and enforces number of US economic and trade sanctions. These sanctions are based on US Foreign policy and national security goals against targeted foreign countries and regimes, terrorists and many others that are engaged in illicit activities. Under presidential national emergency, OFAC takes measures against foreign countries and doubtful organizations such as terrorist groups or certain individuals considered as a serious threat. OFAC is empowered to impose penalties against whoever defies it what involves enormous fees or freezing assets. OFAC rules are applicable on *US persons* that include:

- US citizens, wherever located.
- Permanent US resident, wherever located.
- Entities organized under US law.
- All entities and persons located in the US.
- Entities owned or controlled by US citizens.[81]

It is interesting to mention that the US reached an agreement with Iran in January 2016. In exchange for curbs on its nuclear program, the US has amended some of the nuclear-related secondary sanctions generally aimed at non-US persons (in addition, all nuclear-related

[80]Sanctions policy. www.eeas.europa.eu [online]. 2016 [cit. 2016-09-01]. Available from: https://eeas.europa.eu/topics/sanctions-policy/423/sanctions-policy_en

[81]Office of Foreign Assets Control (OFAC). *www.treasury.gov* [online]. 2015 [cit. 2016-09-02]. Available from: https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx

economic and financial EU sanctions against Iran have been lifted as well). Let us know demonstrate the most relevant aspects of this important step towards the Iran's future:

- Nearly 400 individuals and companies (including banks) fell from the list of targeted persons.
- Oil and gas (and their derivatives) extracted or produced in Iran can be traded on world commodity markets.
- Iran's banks can re-join the SWIFT.
- Possibility to again dispose of the accounts of sanctioned individuals and trade with these persons.

Again, the release of sanction measures by the US relate exclusively to non-US persons, outside US jurisdiction. In other words, EU financial institutions are free to process transactions with Iran and conduct wide range of businesses in Iran's finance and energy segments. However, some of the secondary sanctions has been lifted, it must be said that the US primary sanctions remained, besides of three very limited exceptions. [82]

The US secretary of State John Kerry statement clarifies it all: "*Banks in Europe are allowed to open accounts for Iran; banks in Europe are allowed to do business; banks in Europe can fund programs, lend money"*[83]. Then, why there is still a high reluctance on the part of European banks to process Iranian payments or in general participate financially in Iranian affairs? Since it is a very delicate subject that concerns number of possible causes, we have attempted to encapsulate eventual reasons that discourage European banks from elaborating with Iran:

- As it will be explained in the next chapter, the FATF stills views Iran as a jurisdiction with strategic AML/CTF deficiencies and still monitors its progress in implementing the Action Plan. As the FATF is still worried about the TF risk that Iran possibly poses, there is no surprise that European banks are hesitant in this matter.
- BNP Paribas, French multinational bank, violated sanctions against Sudan, Cuba, and Iran and had to face penalties of nearly 9 billion $ what taught us that fines related to the violation of these sanctions can be tremendous. This makes other banks nervous and very careful.

[82]For European banks, US assurances on Iran come with asterisks. *www.reuters.com* [online]. 2016 [cit. 2016-09-03]. Available from: http://www.reuters.com/article/us-usa-sanctions-iran-idUSKCN0Y92WI
[83]Ibid. (82)

- There are many more regulatory authorities, besides OFAC, that can sanction for the same misdeed. Therefore, banks simply fear to be the first to test the authorities' response.
- The Iranian Revolutionary Guards are being sanctioned as terrorists and own a considerable amount of the Iranian economy. It is then very difficult to operate in Iran, which again leads to unwillingness to face such a risks.
- In reality, the reach of OFAC is much wider and it applies to all transactions that have a link to the US. To be more precise, when the transaction has anything to do with US, such as it is denominated in US dollars, or being handled by a US bank or there is use of US technology, OFAC can apply. Consequently, European banks are still quite hesitant to carry out any businesses with Iran because it is challenging to decide whether there is violation of OFAC rules or not, even if engaging in entirely European transactions.
- Finally, the US Sanctions are extensive and complicated consisting of a comprehensive web of laws so the misinterpretation is another fact that concerns them.

The release of sanction measures by the EU and the US can be classified as their suspension, but not abolishment. The objective of OFAC is to ensure that no sanctioned countries, entities or individuals are engaged improperly in US dollar denominated transactions. OFAC is extremely proactive and diligent in enforcing US policy and thus everybody interested must consider very carefully the impact of any US sanctions on their business activities. Most of the US sanctions are far more aggressive than the sanctions imposed by the UN Security Council or the EU.

As it is evident from the text, OFAC rules can have a huge impact on global business and financial institutions. It is mainly because large proportion of international trade is in US dollars. However, as we have learned, even when a transaction is not conducted in US dollars, it can be subject to OFAC rules.

4.4 The Wolfsberg Group[84]

The Wolfsberg Group is a non-governmental alliance of 13 global banks founded in 2002 that seeks to develop frameworks and guidance for the management of financial crimes, especially regarding AML/CTF measures. The initial idea was that if the key US and European banks get together to work on AML standards, it can be advantageous for both, the banking sector and society. As a first step, the two major banks decided to share their own private AML standards at its first meeting. The group has issued 14 documents so far, named the "The Wolfsberg Standards", with the first regarding AML measures in private banking in 2002. The list of all these standards brings the idea in what areas the Wolfsberg Group operates and it can be found in appendix.

The potency of these standards comes from the fact that member banks are committed to implement the rules to all their operations both at home and abroad (including offshore centers). If we assume, that the member banks create more than 60 % of the world market in private banking, these standards then have a great potential to become leading principles in the banking industry. Furthermore, it should be remembered that the requirements established by FATF throughout its recommendations are aimed at national supervisors and are guidelines of minimal regulatory standards. Besides, the implementation takes time and this time lag is surely one of the factors that prompted banks to be more active.

More simply put, the question of trustworthiness has become primary since the nature of this business requires maintaining the confidence of depositors, creditors and in generally the marketplace. Hence, it is no surprise that banks do not want to wait for the gradual, piecemeal legislation.

[84]The Wolfsberg Group. *www.wolfsberg-principles* [online]. 2016 [cit. 2016-09-04]. Available from: http://www.wolfsberg-principles.com/index.htm

5 Leading macroeconomic indicators

Successful fight against ML/TF certainly requires some estimates to have an idea what we are dealing with but since it is almost unfeasible, from our point of view, responsible authorities should focus their attention mainly on leading indicators as it enables them effectively address this issue. Since we dispose of useful information and assumptions, we believe that a compilation of a list of leading indicators can considerably help in creating most effective countermeasures in all directions. Within this chapter, we have attempted to unite three macroeconomic indicators that we believe facilitate this phenomenon. Their nature and characteristics allow establishment and development of either criminal activities or consequent ML:

- Offshore financial centres.
- Insufficient AML/CTF legislation.
- Leaders in drug trade.

5.1 Offshore financial centres

Offshore financial centres (OFCs) are part of the global economy and play an indispensable role. Irrespective of arguments that OFCs have nothing to do with ML nowadays, we still believe that they facilitate tax avoidance, flight of capital, degradation of regulation, instability and ML as well. First of all, it was inevitable to shortly outline what hides under the term of OFCs. At its simplest, they can be viewed as:

- Jurisdictions that focus primarily on financial services and provide services principally for non-residents.
- Jurisdictions that attract assets mainly by offering low or zero taxation, very moderate regulation, anonymity and *bank secrecy.*
- Jurisdictions where government is to some extent invulnerable to external pressures.
- Jurisdictions where economic growth is extensively dependent on financial services.[85]

[85]IPAS, Roxana. Money laundering through offshore areas. In: *Annals of the University of Petroşani, Economics*, [online]. 2009 [cit. 2016-09-10]. Available from: http://upet.ro/annals/economics/pdf/2009/20090209.pdf

Nevertheless, this broad definition might be very misleading. As many identify offshore centres with islands of small population, it can be easily forgotten that some OFCs are jurisdictions with well-developed infrastructure and financial markets. With respect of above-mentioned, it should be said that in all jurisdictions, transactions that have offshore characteristics can be found.[86]

Financial secrecy index (FSI) ranks jurisdictions based on their secrecy and offshore activities and provides a list of countries considered an OFC. FSI is a tool that aids to understand global financial secrecy, tax havens, illicit financial flows and so on. The following table provides an overview of the 16 biggest OFCs according to FSI in 2015.

Table 7: 16 bigget OFCs according to FSI 2015

Switzerland	**Germany**
Hong Kong	Bahrain
USA	UAE- Dubaj
Singapore	Macao
Cayman Islands	Japan
Luxembourg	Panama
Lebanon	Marshall Islands
The UK	Jersey

Source: Financial secrecy index (22)

Bank secrecy is a legal principle that allows banks to protect personal and account information about their clients. It was created by Swiss secrecy act in 1934 and for its concealed nature, it is considered by many a principle instrument that drives tax evasions, organized crime, bribery, embezzlement, ML and many more. It might be surprising but bank secrecy in Europe has existed for many years because it was well-realized by many European bankers that what money mostly needs is silence, secrecy and reliability.[87]

[86]Offshore Financial Centers. *www.imf.org* [online]. [cit. 2016-09-10]. Available from: https://www.imf.org/external/np/mae/oshore/2000/eng/back.htm#II_A

[87]Bank secrecy. *www.swiss-privacy.com* [online]. [cit. 2016-09-11]. Available from: https://www.swiss-privacy.com/bank-secrecy.html

That being said, it appears that this tradition will be undermined as the Organisation for Economic Cooperation and Development (OECD) has rolled out a system of automatic exchange of information (AEOI) with first information exchanged in 2017. AEOI is a system that requires states to exchange non-resident financial account information. This is assumed to lessen tax evasions and consequently ML needs. So far, more than 100 states have committed to implement it. Moreover, the FATF also urges that jurisdictions should ensure that bank secrecy laws do not prevent recommendations from being implemented.[88] Only one state has not committed to implement AEOI- the US. FSI has stated that US is country of the greatest concern and it is one of the few that has even worsened its secrecy index, moving from 6th to 3th place from 2013 in comparison with other jurisdictions that, on the contrary, have improved their secrecy score.[89]

Precedent text aimed at presenting important step that has been taken and together with fourth AML Directive that brought the requirement of national register of beneficiary owners, we should suppose that the era of banking secrecy is hopefully ending. In the appendix, reader can find a whole list of jurisdictions that have committed to AEOI. Among them, there are number of traditional offshore centres such as British Virgin Islands, Andorra, Isle of Man, Monaco and many more. The question remains how it affects the issue of ML. The issue of ML and tax evasions is a hot topic because there have been many debates whether ML law enforcements should relate to tax crimes. For our purposes is determining that the FATF (and consequently fourth AML Directive) expanded the scope of ML offences by including tax frauds. That is to say, jurisdictions must treat tax crimes as predicate offences for ML. Mentioned policies will partially reduce tax frauds and are a great step towards better transparency but in terms of ML, the problem goes far beyond taxes. This is crucial for us and that is why the OFCs should still stay under the great supervision of authorities. We also believe that traditional perceptions that OFCs are only sunny exotic islands divert public's attention from the fact that actually big economies such as Germany or the US are becoming leaders in offshore business. According to FSI, Germany has flown under the radar for several years and it is time to admit that is also causing a threat. Not only

[88]Standard for Automatic Exchange of Financial Account Information. *www.oecd.org* [online]. [cit. 2016-09-11]. Available from: https://www.oecd.org/ctp/exchange-of-tax-information/automatic-exchange-financial-account-information-common-reporting-standard.pdf

[89]Financial Secrecy Index 2015 reveals improving global financial transparency, but USA threatens progress. *www.taxjustice.net* [online]. [cit. 2016-09-16]. Available from: http://www.taxjustice.net/wp-content/uploads/2013/04/FSI-2015-Presser.pdf

does it not sufficiently share tax-related information, is characterized by negligent AML regime and offers an alarming set of secrecy instruments such as bearer shares (there were certain amendments in 2015) but also it is not so long ago when also the FATF made some serious concerns about the use of entities such as trusts, Treuhand and foundations in Germany. As we have outlined earlier in this chapter, the situation is very similar in case of the US that takes the third place within the list. It is no news that the US has been taking serious measures to defend itself from tax havens, attacking very aggressively the Swiss banking establishment and even creating Foreign Account Tax Compliance (FATCA) that requires foreign financial and some non-financial institutions to report on foreign assets held by American citizens. For this reason, it is very worrying that now, according to FSI, the US accounts for one fifth of the global offshore financial activities, exchange very little information with other countries in return and offers wide range of secrecy together with some tax-free facilities for non-residents.[90] Does it not meet the definition of OFC?

To summarize this complex issue, we have broached, we would like to repeat that the traditional stereotype that most OFCs happen to be the least populous palm-fringed sunny islands is obviously becoming out of date. The truth is some OFCs actually are world's biggest and wealthiest countries. This should be surely borne in minds of regulatory authorities. Besides, tax fraud surely is profit of illegal activity that requires laundering, but as we know, it accounts for only part of proceeds of crimes. With this in mind, bank secrecy is staple of many jurisdictions, including offshore banking sectors. It contributes to ML by blocking the free flow of information inevitable to identify rogue foreign banks and criminals seeking to misuse the correspondent banking system to launder illegal funds. Furthermore, bank secrecy undermines law enforcement and regulatory efforts. In short, money launderers thrive in bank secrecy jurisdictions that impede disclosure of their accounts and activities. Therefore, there should be more and more efforts to confront secrecy.

[90]Financial Secrecy Index. *www.financialsecrecyindex.com* [online]. [cit. 2016-09-18]. Available from: http://www.financialsecrecyindex.com

5.2 Insufficient AML regimes

Following text has built on the facts mentioned in the subchapter dealing with the role of FATF. As we know, the FATF surely is the most influential policy-making body whose aim is to not only combat ML/TF but also supervise the countries' AML/CTF regimes and lead them to achieve satisfactory outcomes. For this reason, we have relied on the evaluations undertaken by this authority and determined the risky jurisdictions based on it.

We have a general idea about the nature of the FATF blacklisting from the chapter dedicated to combating ML/TF. The logic behind the FATF "blacklist" is that it tries to hunt non-cooperative countries with the aid of a "name and shame" policy. This year's third plenary meeting was held in Paris, under the Spanish Presidency of Mr Juan Manuel Vega-Serrano. The delegates discussed issues regarding TF, which is right now the FATF top priority. In addition, two public documents identifying countries that may represent a risk were published. The text below yields this year's revision of jurisdictions that fall into a certain category according to which they have to undertake certain steps and fulfil specific requirements.

Countries subject to a FATF call on its members and other jurisdictions to apply sufficient countermeasures in order to protect the international financial system from ML/TF risks:

- Iran.
- North Korea.

We are not capable of discussing every single country per se and circumstances that led to their inclusion under one of these categories. Despite that, we believe it is in place to demonstrate at least cases of Iran and North Korea that were blacklisted and thus marked as high-risk jurisdictions:

- *Iran* will be part of the FATF public statement until the action plan has been fully conducted. Iran is mainly urged by the FATF to take action in the matter of addressing AML/CTF weaknesses, particularly those concerning TF. Rather than removing Iran from the backlist, the FATF has temporally suspended countermeasures for next 12 months to monitor its progress which indicates that it still has a very long way to go before it is considered safe to do business there.

- *North Korea* remains under the supervision of the FATF because of its failure to deal effectively with deficiencies within its AML/CTF regime what, as we already know, hinder the integrity of international financial system. Besides, the FATF is highly worried about the menace of North Korea's illegal activities regarding proliferation of weapons of mass destruction.[91]

Countries, which have certain strategic AML/CTF deficiencies due to which they have taken measures such as action plan:

- Afghanistan.
- Bosnia a Herzegovina.
- Iraq.
- Lao PDR.
- Uganda.
- Yemen.
- Vanuatu.

For a better idea, and at the same time with a certain generalization, we can sum up that these jurisdictions are monitored mostly because of following matters:

- Inadequate criminalising of ML/TF.
- Inadequate framework needed for identifying, tracing and freezing terrorist assets.
- Necessity to implement supervisory and oversight programme for financial sectors.
- Need to develop channels for international cooperation and national coordination policies.
- Absence of fully operational financial intelligence unit and better transparency
- Necessity to strengthen preventive measures, including wire transfers for instance.[92]

Aforementioned deficiencies and requirements differ in terms of each jurisdiction and it is understood that some of these shortcomings are elementary. Furthermore, it should be stressed that considerable number of jurisdictions have not been reviewed yet but the FATF continues in identifying other countries that represent a risk. This should be very well-

[91]Public Statement - 24 June 2016. *www.fatf-gafi.org* [online]. [cit. 2016-09-20]. Available from: http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-june-2016.html
[92]Ibid. (91)

remembered because countries we have brought to attention surely suffer from certain AML/CTF shortages but we cannot exclude the fact that there are other risky countries not yet examined. Disclosing these jurisdictions should urge other countries to be on guard and take a risk-based approach towards them. The previous indicator surely contains an element of assumption but following conclusions about the quality of AML/CTF regimes observed by the FATF are real and confirmed matters. Therefore, jurisdictions with identified scarcities and deficiencies pose a real threat in terms of facilitating ML/TF and should be under the close examination and supervision.

5.3 Leaders in drug trade

The third factor that tremendously helps create and shape ML concerns organized crime within underground economy. We are of the opinion that organized crime generates extensive ML problems for governments, has vast negative impact on security of individual citizens and communities, causes suffering and undermines further development of countries. The quantity of organized crime may also serve as a further indicator. Put differently, physical location of any kind of crime that generates funds to be laundered can serve as an indicator. Why? Because ML needs in this location can be highly expected.

For this reason, we believe that law enforcements should combat the supply side at the maximum extent and thus control ML at root. Within this subchapter, we have focused merely on the criminal sector of shadow economy, specifically drug trafficking, as it has profoundly disastrous social consequences and together with fraud yields most of illicit proceeds. One utterly critical step in the illicit drug trade is the process of laundering vast amounts of cash into usable assets. The below statement, from the drug trafficker perspective, clarifies it perfectly:

"It became more of a problem to count the money and stack it. I mean, it took hours upon hours and hours to do it and recount it and go over and over it again. It was tedious as hell. Money became an obstacle. You know, it started to take the fun out of the whole thing, believe it or not."

George Jung

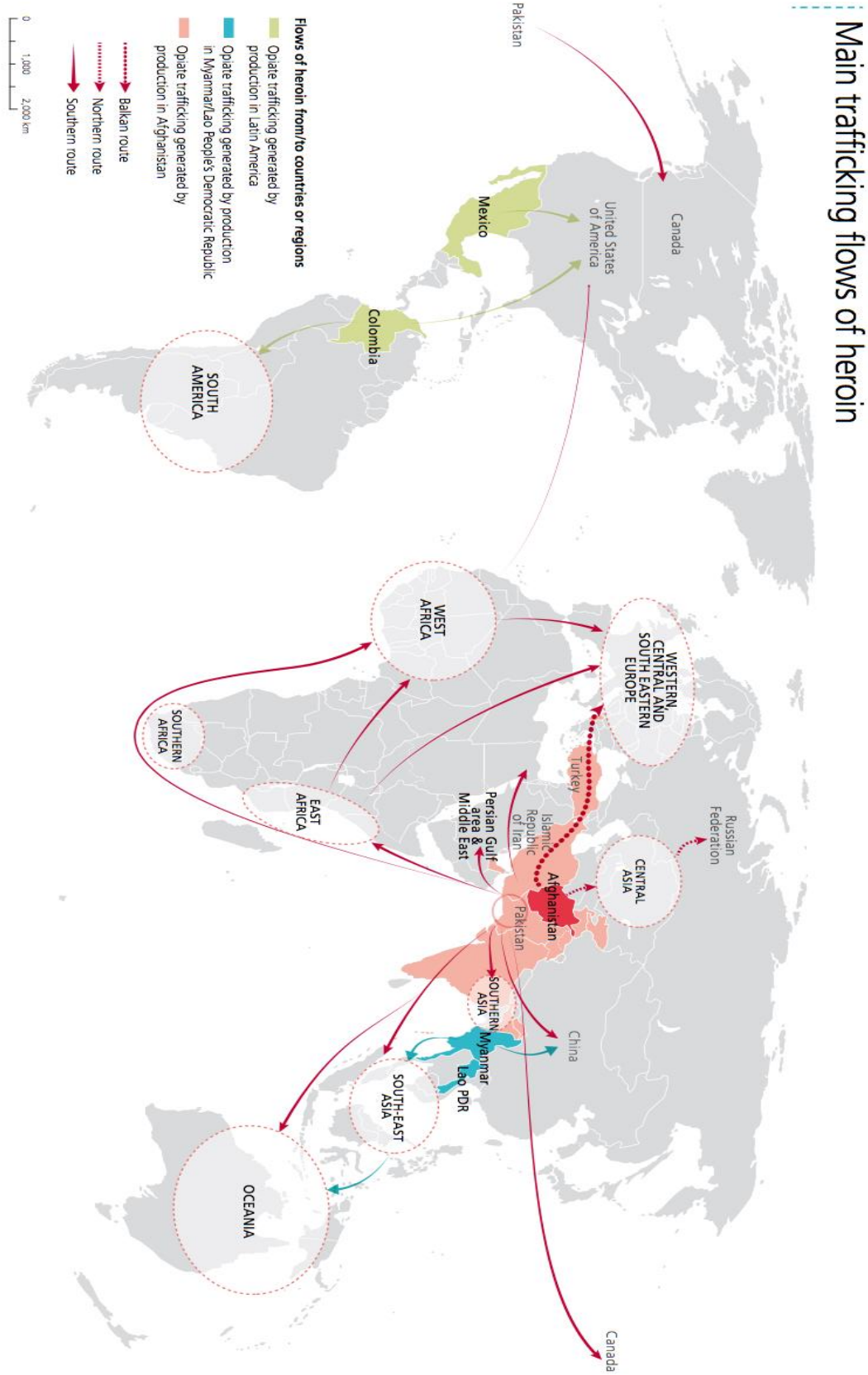
Drug trafficking involves the manufacture, distribution and consequent sale of drugs. The role of drug trafficking in context of ML is immense and that is why it is the activity that is the most related to ML. For a long time, law enforcement concerning AML focused predominantly on drug trafficking. Even if it is understandable, it is highly inaccurate, mainly at present when also frauds evolve. Today's AML regimes concerns variety of illegal activities but it must be admitted that drug trafficking plays particular role and it is one of the world's major issues. Laundering of drug money does not represent specific approach and does not really differ from traditional ML. However, it should be noted, that since vast amount of money is involved in drug trade, launderers usually move to other sectors than banking, seeking less supervision.[93] Drugs come in wide range of forms. Some are legal and others illegal. There are eight key categories of drugs that are produced:

- Stimulants- *Cocaine*, Methamphetamine…
- Opioids & Morphine Derivatives- *Heroin*, Morphine, Opium…
- Cannabinoids- Hashish, Marijuana…
- Depressants.
- Anabolic Steroids.
- Hallucinogens.
- Inhalants.
- Prescription drugs.

The following text has focused merely on illegal drugs, specifically heroin and cocaine trafficking as cocaine and heroin may be regarded as two of the most addictive substances around. We have attempted to determine high-risk countries based of available information. Following two pictures demonstrates heroin and cocaine market.

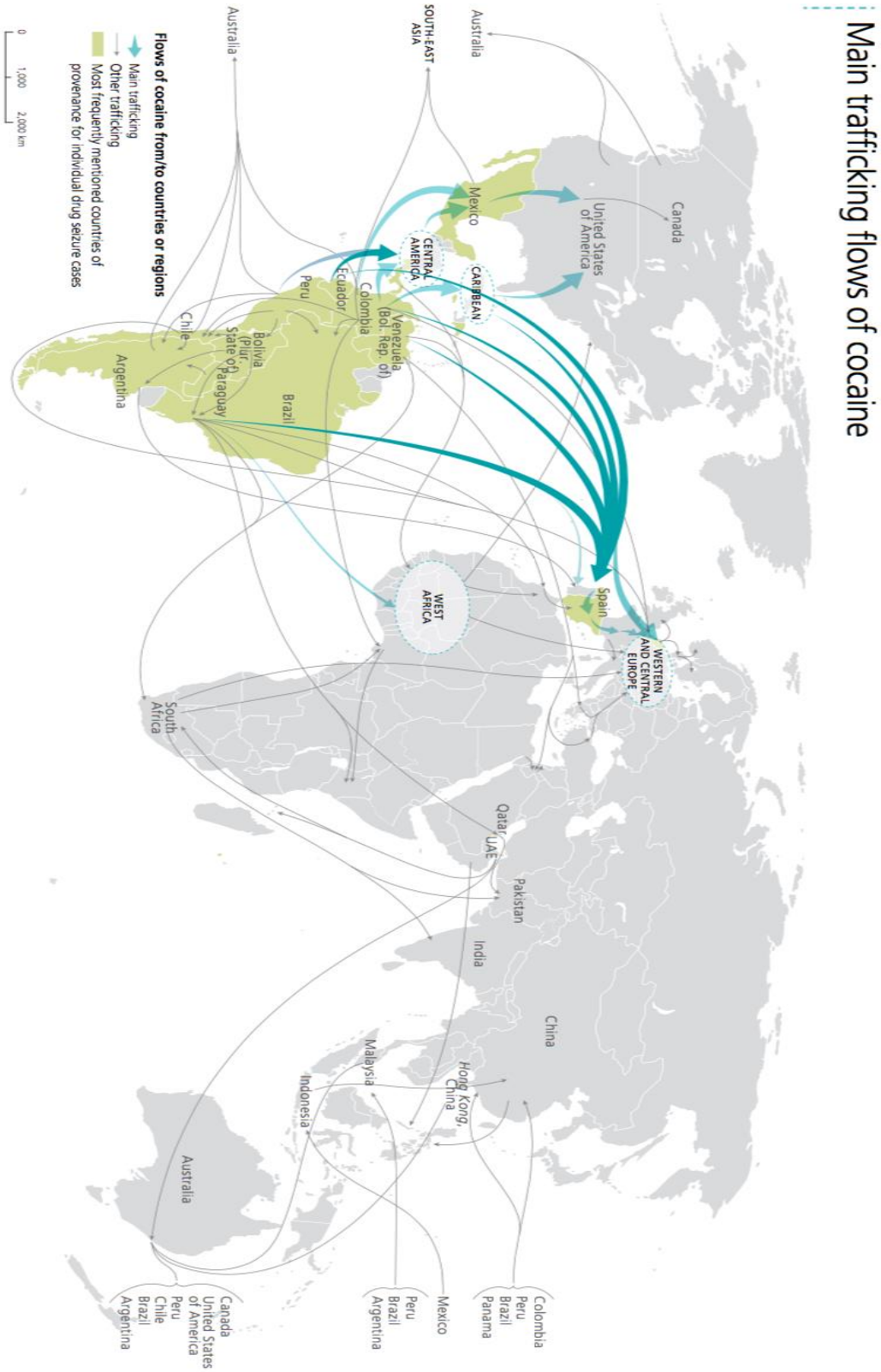
[93]Illicit trafficking in narcotic drugs and money laundering. *www.menafatf.org* [online]. 2011 [cit. 2016-09-21]. Available from: http://www.menafatf.org/images/UploadFiles/Illicit_Trafficking_and_ML_Eng.pdf

Picture 5: Heroin market



Source: UNODC, (83)

Picture 6: Cocaine market



Source: UNODC, (83)

Table 8: Top 10 heroin trafficking countries

Afghanistan	Netherlands
Pakistan	Iran
Tajikistan	India
Albania	Thailand
Turkey	Kirghizstan

Source: www.therichest.com, (1)

Above list of countries represents the ranking of the top 10 heroin trafficking countries with *Afghanistan* at the top.[94]Although, the global opium[95] production in 2015 declined by 38 % which was a consequence of the decrease in production in Afghanistan, this country still represents the main source of the world south Asian opium. Besides, it is also where the famous Balkan Route starts through which Western and Central Europe is supplied. In addition, previous subchapter has taught us that Afghanistan still experiences AML/CTF deficiencies and thus remains under the monitoring of the FATF. This, together with its irreplaceable role in heroin trafficking established Afghanistan a worldwide threat not only in terms of organized crime but also ML/TF.[96] However, it is supposed that most proceeds of drug trafficking are laundered outside of the country, the key here is that drug trafficking evokes the whole process of laundering. Additionally, HAWALA system presented in first chapter is actually the most effective and sometimes the only way to move money in the country. For this reason, we cannot suppose that it is used solely for transferring illegal proceeds within drug trafficking or TF. Having said that, HAWALA certainly is appealing to Afghan drug traffickers to disguise ill-gotten gains from the government. Therefore, we strongly believe that Black HAWALA is at the center of Afghanistan's problem with ML/TF.[97]

However, *Iran* does not produce almost any of its own opium, it represents the country with the highest per capita drug use. It is probably because the primary conduit for drug

[94]10 Biggest Heroin Trafficking Countries In The World. *www.therichest.com* [online]. 2014 [cit. 2016-09-21]. Available from: http://www.therichest.com/rich-list/the-biggest/the-10-hottest-countries-in-heroin-trafficking/

[95] Heroin is made from opium but opium is not the same thing as heroin.

[96]World Drug Report. *www.unodc.org* [online]. 2016 [cit. 2016-09-21]. Available from: https://www.unodc.org/doc/wdr2016/WORLD_DRUG_REPORT_2016_web.pdf

[97]Dirty Money in Afghanistan: How Kabul is Cleaning Up the Illicit Economy. *Www.foreignaffairs.com*[online]. 2016 [cit. 2016-09-23]. Available from: https://www.foreignaffairs.com/articles/afghanistan/2016-09-07/dirty-money-afghanistan

trafficking, the Balkan Route, passes through Iran from Afghanistan and thus it is a key transshipment point for Southwest heroin. The fact that Iran shares over 1 500 km common border with Afghanistan largely facilitates the whole trafficking. Furthermore, Iran occurs on the FATF blacklist, which signalizes very large AML/CTF inadequacies and thus includes Iran among the high-risk jurisdictions.

Between years 2009-2014, 153 countries reported cocaine confiscation. As it is very well-known, most cocaine trafficking comes from South America. Andean states, such as *Colombia*, Peru and Bolivia, still function as the biggest cocaine suppliers for North America and Europe but as it is clear from the picture 6, Central America and Caribbean countries are involved too, although mainly as transshipment locations. The latest survey done by United Nations Office on Drugs and Crime (UNODC) showed an increase of almost 40 % in the coca crop area - from 69 000 ha in 2014 to 96 000 ha in 2015. Additionally, and more alarmingly, this figure is twice the size of the coca cultivation surface in 2013, which was of "only" 48 000 ha.[98] The point for us in terms of ML is very clear and scary at the same time: The increased coca cultivation is very likely to provide transnational organized crime with injection of cash that subsequently becomes part of the laundering roll coaster. What is more, it is still considered an underestimation of the real amount that is produced each year in Colombia.

Columbia is a member of the Financial Action Task Force of Latin America (GAFILAT). GAFILAT is also committed to perform mutual evaluation similarly as FATF. The latest mutual evaluation was conducted in Colombia in 2008. The assessment of Columbia's AML regime revealed some serious shortages such as no obligation for lawyers to report suspicious transactions or no enhanced due diligence for PEPs.[99] As far as we know, there were no significant amendments and thus Columbia remains to pose real risk in both organized crime and ML. Furthermore, we assume that mentioned BMPE, as a trade-based laundering, still fuels laundering of drug money. Juan Ricardo Ortega, the head of the Colombian tax and customs agency, between years 2010 and 2014, hit the nail on the head

[98]Monitoreo de territorios afectados por cultivos ilícitos 2015.*www.unodc.org* [online]. 2016 [cit. 2016-10-05]. Available from: http://www.unodc.org/documents/crop-monitoring/Colombia/Monitoreo_Cultivos_ilicitos_2015.pdf

[99]Colombia. *www.Anti-Moneylaundering.org* [online]. 2014 [cit. 2016-10-06]. Available from: http://www.Anti-Moneylaundering.org/southamerica/Colombia.aspx

and said: "*The peso brokers who aid to launder money are as vital to the drug trade as the chemicals used to process coca leaves into cocaine.*" [100]

Even if we have put emphasis mainly on Colombia, the problem of drug trafficking and related ML is without doubt problem of other Latin American states too. Because of Colombian anti-narcotic strategies, Colombian Cartels are not as powerful as they were back in 90s. The most influential Drug Cartels are now located in *Mexico***.** Mexico does not belong to the top producers of the coca but these Cartels purchase cocaine processed in South America, mostly in Colombia and then smuggle it into the US to sell. It seems like Colombia-Mexico drug alliance, giving rise to the international ML, requires separate but coordinated anti-narcotics responses. On the one hand, elimination of the Mexican Drug Cartels, and on the other, decreasing the coca cultivation of the largest producer, Colombia. Successful Drug War will largely contribute to war against ML as well. The connection is undoubted.

An incredible example that bridges over drug money and ML through banking sectors and is relevant at this point can be illustrated through briefly outlined HSBC case in box 1.

Box 1: Case of HSBC

HSBC Bank USA, N.A. (HBUS), the US subsidiary of HSBC Group, providing correspondent banking accounts to its sisters located in other countries failed to monitor more than 670 billion $ in wire transfers and more than 9.4 billion $ in purchases of US currency from HSBC Mexico, between years 2006-2009. Thus, it was estimated that at least 881 million $ coming from the drug trade Mexico's Sinaloa cartel and Colombian Norte del Valle were laundered. This is the first case in which the banking institution openly admitted to ML. The case concerns wire transfers and foreign exchange transactions but with increased pressure, Cartels might use more complex methods involving securities in the future.

Source: www.reuters.com, (30)

The point of this example is to highlight the importance of the fact that enhancing regulatory requirements towards banks is a necessity but it is also critical and equally important to

[100]Colombia's Discount Currency Exchanges Are Funnelling Drug Money. *www.bloomberg.com* [online]. 2016 [cit. 2016-10-07]. Available from: http://www.bloomberg.com/news/articles/2016-01-28/cocaine-s-unbroken-grip-on-currency-market-trading-in-colombia/Colombia.aspx

provide more than sufficient supervision of banks and their procedures within AML/CTF. The example shows that the world can spend billions of dollars combating this damaging threat but it is all useless unless financial institutions, the absolute fundament of this whole fight, do not fully participate in it.

Obviously, all mentioned jurisdictions deserve great attention as they represent the root of drug-ML. At some time in past, drug trafficking was limited to certain number of countries. Now, it touches the whole global community and jurisdictions not influenced by drug trafficking are sadly only exceptions. As a result, it surely is difficult to use drug trafficking as a leading indicator. However, we can certainly come to conclusion that countries labeled as top drug problematic must be kept under the very close monitoring, as well as banks operating in these countries. Moreover, it is to be noted, that since there is surely no doubt that fighting ML/TF helps reduce significantly international crime rates (and consequently repeated ML), jurisdictions must ensure that sufficient coordination is undertaken between bodies involved in combating drug trafficking on one side and agencies concerned with ensuring adequate AML/CTF regimes on the other. They both can highly contribute to each other's researches.

6 Bank's procedures within Anti-money laundering in Czech Republic

Previous chapters have intended to provide complex understanding of ML at a macro level. Now, as we dispose of sufficient knowledge, we are close from concluding this issue. The very end of this comprehensive subject should be successful response of financial institutions throughout AML/CTF measures.

Not to speak about AML/CTF procedures in generally, this chapter has required specific aim and that is to deal with AML/CTF regime from perspective of selected jurisdiction, namely Czech Republic (CR). CR is a very good choice due to several aspects. Its combination of economic and geographical factors makes it a location for transnational crime[101] and as CR remains a predominately cash intensive economy, it is a vehicle for ML. The objective at this point was to offer general illustration of concrete AML/CTF measures and not to go in very little details by evaluating the quality of them.

CR, as a member of EU, must comply with mentioned AML Directives and provide their implementation within its own AML/CTF legislation. The primary national act that regulates this issue is Act No. 253/2008 Coll. 19 October 2016 on selected measures against legitimisation of proceeds of crime and financing of terrorism (new amendment of the act came to force 1 January 2017). As we have highlighted, the fourth AML Directive was adopted in May 2015. Due to this, transposition was needed, addressing also several amendments that EC proposed this year. The Act applies to several obligated entities but we merely considered banks. The Czech National Bank is responsible for monitoring compliance with obligations laid down under AML/CTF act and regularly supervise liable persons. One of the major risks that banks and other financial institutions face is the reputational risk. The use of banking system for ML/TF has been mentioned many times and thus it is obvious that financial institutions are constantly put at risk.

Most of the relationships between bank and customer begin with an account-opening procedure. The information gathered and verified at this point is key to the bank in order for

[101]Particularly drug trafficking from the Balkan region, Middle East and South Asia.

it to meet its AML/CTF obligations. There are two crucial legal and regulatory obligations regarding individual employee's perspective:

- Know Your Customer (KYC).
- Reporting of suspicious transactions.

6.1 Know Your Customer

KYC is the very first line of defense against ML/TF intensions and thus it is of critical importance for any financial institution. As the name indicates, its primary goal is identification and consequent verification of a customer but it includes all other processes discussed later. To have a clearer idea and grasp the AML process well from the beginning, it is beneficial to divide KYC into these principle parts:

- Customer Identification Program (CIP).
- Customer Due Diligence (CDD).
- Customer categorization in terms of risk factors.
- Monitoring customer transactions.

CIP is an initial step and a mandatory requirement that needs to include all following steps to be carried out correctly:

- To collect information about clients.
- To verify this information. Verification must be performed prior to the establishment of relationship with client.
- To carry out the sanction screening. This refers to sanctions mentioned in chapter 4. Financial institutions are required to screen their new customers against sanction lists that might be applicable when starting new relationship and then on certain periodic basis.[102]
- Record keeping.[103]

CDD includes number of measures and comprises information about clients enabling to evaluate the risk they hold. While some of these measures apply at the beginning of the

[102]Banks in the CR, in generally, are under a legal obligation to apply each sanction as prescribe, whether that involves freezing assets or denying wire transfers. They are mostly directly affected by the sanctions imposed by the US, the EU and the UN.
[103]Customer Identification Program (CIP). *www.advisoryhq.com* [online]. 2016 [cit. 2016-11-01]. Available from: http://www.advisoryhq.com/articles/developing-a-well-defined-customer-identification-program-cip/

relationship, others are carried out continuously throughout the relationship. This implies that it is an on-going process and the core of AML practices. CDD may be:

- Simplified.
- Standard.
- Enhanced.[104]

Enhanced CDD provides financial institutions with more detailed background check of certain individual and thus helps mitigate increased risk of ML/TF. It is paramount to note that according to the FATF and the fourth AML Directive, all jurisdictions should apply risk-based approach as it enables them to use measures that are more flexible and address possible ML/TF risks in the most effective manner. What does it mean in practice? Risk-based approach asks for enhanced CDD in any case that represents greater risk. Many situations can be considered high-risk. Following two examples can be offered:

- Dealing with PEPs.
- Dealing with clients not face to face. This situation can easily arise from Internet or telephone banking.

On the other hand, risk-based approach allows usage of standard CDD for low-risk clients such as public authorities, listed companies or regulated financial companies.

According to the decree No. 281/2008 on selected requirements regarding the system of internal principles, when assigning a risk status of a new client or updating the inclusion of existing client under certain risk category, bank should evaluate a degree of risk at least with respect to:

- The fact that some countries of origin of the client might insufficiently or at all apply measures against ML/TF.
- The fact that person, with whom the client does business, comes from a country with a lack of appropriate measures against ML/TF.
- The fact that client, or the person with whom the client does business is subject to sanction in accordance with legislation.
- Non-transparent ownership structure of the client.

[104]KYC/AML/CTF/International Sanctions Program. *www.unicredit.ro* [online]. 2016 [cit. 2016-11-03]. Available from: https://www.unicredit.ro/content/dam/cee2020-pws-ro/DocumentePDF/Banci-corespondente/KYC_AML%20Policy%20UCT.PDF

- The unclear origin of the funds.
- The facts giving rise to the suspicion that the client does not act on his own behalf or obscures that is fulfilling the instructions of the third persons.
- Unusual trade execution, particularly with regard to the type of client, subject, amount, the purpose of the business relationship and the subject of client activity,
- The facts suggesting that the client carries out a suspicious transaction.
- The fact that according to the information available to the institution is subject to the client's business linked to an increased risk of ML/TF.[105]

In order to determine a customer's total risk rating, a selected list of customer variables are evaluated and each variable is then scored with a low, medium or high-risk. Among various variables, the type of business plays an essential role in terms of corporate clientele. Various risky businesses may serve as vehicles for ML/TF. These include businesses in which there is a scope for tax evasion (products that are subject to excise taxes), mixing of illicit funds with legal sales (travel agency, restaurants) or industry easily misused to provide fictitious and overvalued services (consulting). Caution must be given to fields with the possible involvement of criminal organizations (production of weapons and ammunition, casinos).

Apart from the above-mentioned client identification, a bank must prior to a single transaction amounting to 15 000 € or more perform CDD.[106] It means that client must submit any information and documents inevitable for the due diligence including:

- Information on the intended nature of the transaction or business relationship.
- Identification of the beneficial owner, should the customer be a legal person.
- Information that are necessary for on-going monitoring of the business relationship, including scrutiny of transactions conducted during the course of that relationship to ensure that the transactions are identical with the institution's knowledge of the customer, its business and risk status.
- Examining the sources of funds.

[105] No. 281/2008 Coll. of 25 June 2014 on certain requirements for the system of internal principles, procedures and control measures against money laundering and terrorist financing. Available from: http://www.epravo.cz/top/zakony/sbirka-zakonu/vyhlaska-ze-dne-25-cervna-2014-kterou-se-meni-vyhlaska-c-2812008-sb-o-nekterych-pozadavcich-na-system-vnitrnich-zasad-postupu-a-kontrolnich-opatreni-proti-legalizaci-vynosu-z-trestne-cinnosti-a-financovani-terorismu-20119.html, § 2

[106] In addition, when dealing with PEPs and a person established in the country that based on indications of the European Commission or any other reason must be considered a high-risk.

- In case of a business relationship with a PEP also reasonable steps to identify the origin of its assets.[107]

In case of a failure to justify the intention and origin of funds within certain transaction, it is evaluated as suspicious. The refusal on the part of a customer to cooperate is one of the reasons not to proceed the order. Despite of the cooperation, the due diligence process may reveal some unusual attributes and it is thus a candidate for suspicious transaction.

Aside from the issue of ML/TF, internal AML system with its KYC principles plays a key role in other areas of risk management as well. It represents one of many critical elements inevitable for safe and reliable operation of the bank and virtually the entire banking system. KYC goes far beyond a simple account opening and record keeping procedures. It requires banks to formulate a customer acceptance policy and customer identification programme including more extensive due diligence for high-risk accounts. In addition, it involves proactive account monitoring for potential suspicious activities.

6.2 Suspicious transactions

We have learnt that perpetrator that illegally obtained money does not spend them directly but integrate them to legal economy through ML process. Recognizing suspicious transactions is then absolutely critical step to detect and prevent ML/TF. Therefore, banks should keep their staff well-trained so they can identify potentially suspicious transactions or orders as soon as possible.

Suspicious financial transaction is a term that the FATF firstly used in the 40 recommendations. According to AML/CTF act, it is a transaction that possesses features arousing reasonable suspicion of being related to ML/TF. It must be borne in mind that behavior is suspicious, not people. Suspicious transactions comprise both completed and attempted transactions. There are certain attributes establishing reasonable suspicion that there may be a connection with ML/TF. The last chapter is dedicated to presenting these attributes together with the case study of a situation containing several of these features.

[107]Act No. 253/2008 Coll. of 19 October, 2016 on selected measures against legitimisation of proceeds of crime and financing of terrorism Available from: http://www.epravo.cz/_dataPublic/sbirky/2016/sb0147-2016.pdf, § 9

In accordance with AML/CTF act a transaction must always be considered suspicious, should:

- *"the customer or the beneficial owner be a person against whom the Czech Republic has imposed international sanctions under the Act on Implementation of International Sanctions,*
- *the goods or services involved in the transaction fall in the category against which the Czech Republic has imposed international sanctions under the Act on Implementation of International Sanctions,*
- *the customer refuses to reveal identification data of the person they are representing or to undergo the due diligence process in accordance with AML/CTF act."*[108]

Obligated entity, in our case a bank, must report a suspicion regarding certain transaction to Ministry of Finance within 5 days according to the AML/CTF act. Within the Ministry, *Financial Analytical Unit (FAU)* is in charge of this agenda. FAU functions as the CR's financial intelligence unit and primarily handles tasks assigned to the Ministry of Finance under special legislation for combating ML/TF.[109] The bank must provide maximum interoperability and:

- The identity of all the parties to whom/which the report relates.
- Whether the transaction has been completed.
- A description of the subject - matter of the transaction - the reason as to why the reported transaction has been classified as unusual must be always specified.

If there is a reasonable risk that executing the transaction might be thwarted or substantially impede seizure of proceeds from crime, the bank may fulfill the client's order concerning a suspicious transaction no sooner than 24 hours after receipt of the notification of suspicious transactions by the Ministry of Finance. If the investigation requires a longer period to assess and analyze reported transaction, Ministry of Finance has a possibility to extend the delay for the execution of an instruction issued by a customer by a further 48 hours, a total of 72 hours. If the bank is not informed within the aforementioned period (24 hours/72 hours) that the complaint has been filled, the bank executes the order. Otherwise, the bank executes the

[108]Act No. 253/2008 Coll. of 19 October, 2016 on selected measures against legitimisation of proceeds of crime and financing of terrorism Available from: http://www.epravo.cz/_dataPublic/sbirky/2016/sb0147-2016.pdf, § 6,

[109]FAÚ. *www.mfcr.cz* [online]. 2016 [cit. 2016-11-03]. Available from: http://www.mfcr.cz/cs/zahranicni-sektor/ochrana-financnich-zajmu/boj-proti-prani-penez-a-financovani-tero/zakladni-informace

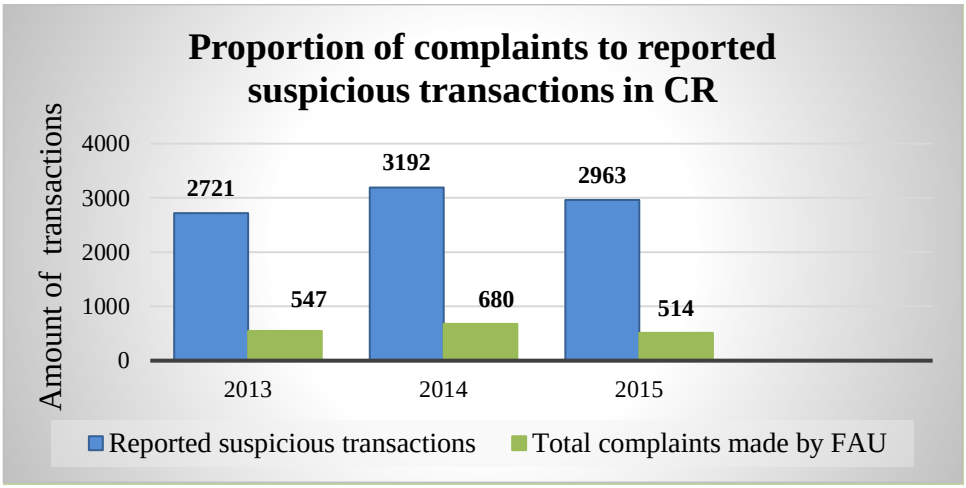
order after 3 days after filing a criminal complaint, unless the competent criminal justice decides on security or withdrawal of such transaction.[110]

A bank has several options how to report an unusual transaction:

- By filling in a Suspicions Transaction Report. FAU created software application MoneyWeb Lite for liable persons. The main purpose of the application is to provide an easy and complete submission of suspicious transactions.
- By email.
- In case of a great emergency, by telephone.

As it was expressed, the FAU deals with every single reported transaction. To have an idea of have many reports it annually receives, see the following graph 2.

Graph 2: Proportion of complaints to reported suspicious transactions



Source: own processing, FAU annual report 2015, (18)

In 2015, FAU received 2 963 notices of suspicious transactions. Compared to 2014, there was decrease by 7 % what it is believed to be a result of enhanced quality of reporting processes and elimination of trivial or insignificant reports. This creates more space for dealing with serious cases of ML/TF. As the graph shows, in 2015, 514 criminal complaints were made and in 294 cases the criminal complaint was made together with securing of funds. Overall sum of secured funds reached 5 542 million Czech crowns. Tax sphere was

[110]Act No. 253/2008 Coll. of 19 October 2016 on selected measures against legitimisation of proceeds of crime and financing of terrorism. Available from: http://www.epravo.cz/_dataPublic/sbirky/2016/sb0147-2016.pdf, § 20

one of the most common areas of predicate offenses in 2015. Other most common predicate offences were bankruptcy, corruption and prostitution. Often, the predicate offences are committed abroad and then there is an effort to invest these funds in the CR. According to FAU, the most common laundering techniques in the CR are:

- Misuse of bank account based on fictitious identity.
- Repeated electronic transfers between CR and abroad.
- An effort to lead out the funds to tax havens.
- Interruption of financial cash flow by repeated withdraws and deposits.
- Misuse of virtual currency and investments in real estate.[111]

A common feature of aforementioned trends is an increasing number of cases with an international element. For this reason, an effective collaboration of all international bodies dealing with AML/CTF is inevitable.

[111]Výroční zpráva FAÚ 2015. In: *www.mfcr.cz* [online]. 2015 [cit. 2016-11-18]. Available from: http://www.mfcr.cz/cs/zahranicni-sektor/ochrana-financnich-zajmu/boj-proti-prani-penez-a-financovani-tero/vysledky-cinnosti-financniho-analytickeh/2015/zprava-o-cinnosti-financniho-analytickeh-24287

7 Leading microeconomic indicators

The chapter highlighting leading microeconomic indicators concludes this diploma thesis that has desired to provide complex overview of ML from macroeconomic and microeconomic perspective. In parallel to chapter 5 that has dealt with leading macroeconomic (global) indicators and suggested that regulatory authorities should approach the issue to some extent from supply side, this chapter, on the other hand, has drawn attention to several leading microeconomic indicators that can be divided into:

- Indicators of suspicious transactions.
- Shortages of bank's AML policies.

Since issue of detecting suspicious transactions is crucial element of successful AML process, we have considered very helpful to model a situation consisting of number of leading indicators that cannot be neglected. Furthermore, we have also brought to the attention common but serious weaknesses in risk assessment policies that have been observed by regulatory authorities within bank's internal systems.

7.1 Indicators of suspicious transactions

To make the detection of suspicious transactions expedient, we have tried to summarize several indicators that establish the suspicion and help track the attempt of ML/TF down. Firstly, transaction can be abnormal with regard to:

- The profile.
- The characteristics.
- The usual transaction pattern of the client.

Unusual transaction can be classified under below listed categories. For each category, several examples are provided. These examples can surely overlap and meet characteristics of several categories:

- **Unusual transactions inconsistent with client's financial standing:**
    - Transactions that do not correspondent with the level of income customer has.
    - Sudden start of making investments to large amounts while it is obvious that client does not dispose of capacities to do so.

- **Large cash transactions:**
  - Settlement of securities in large amount of cash.
  - Depositing large sum of cash in certain banks in one day or in a very short period of time.
  - Exchange or purchase of large amount foreign currency.
  - Purchasing several insurance products in cash within short period of time.
- **Irregular account movements:**
  - Transfer of assets that has no clear financial justification.
  - Holding securities for unusually short period of time.
  - Frequent wire transfers and immediate withdraw of sums.
- **Suspicious behavior:**
  - Client is reluctant to undergo identification process or disclose on behalf of whom he or she is acting.
  - Client is nervous, unconfident and rush when conducting transaction.
  - Client provides fictitious or vague information about his identity or source of income.
  - Use of products contrary to the purpose for which they were created.
  - Number of accounts that does not match with client's objectives or assets.
  - Client opens an account and terminate the contract after a short period of time.
  - Requested import/export payments without all required documents.
  - Client deposits cash that is significantly below the reporting threshold amount on a regular basis, apparently attempting to avoid triggering the identification.
  - Curiosity of how internal system and reporting system work.
- **Dealing with high-risk jurisdictions:**
  - Transferring or receiving money from jurisdictions where drug trafficking or other criminal activities are common.
  - Transferring or receiving money from jurisdictions known as financial secrecy countries or tax havens.

- Transferring or receiving money from countries where AML/CTF measures are not adequately implemented.[112]

The box 2 brings the example of number of transactions that took place in several branches of Bank X within few days.

Box 2: Example of web of suspicious transactions

1.1.2016	Mr. X is an entrepreneur that owns a farm. He set up a bank account with initial deposit of 1 000 €. The account was set up mainly for business transaction purposes. Mr. X resides in a very similar address with Mr. Y that is also a client of this bank.
2.1.2016	General financial directorate issued a tax restitution of company G - it was found out later.
3.1.2016	Consequently, Mr. X received money from the restitution in the name of company G in amount of 55 000 €. It was revealed later that director of company G has some relation with Mr. X.
4.1.2016	Mr. X and Mr. Y came to the bank and withdrew cash in amount of 50 000 € from the account of Mr. X and then following transactions were undertaken: ▪ Mr. Y immediately transferred 25 000 € to his account. ▪ Mr. Y transferred the same amount to other account of Mr. Z. Subsequently, Mr. Y withdrew 20 000 € and conducted following transactions: ▪ Deposited 10 000 € on behalf of account of Mr. Z. ▪ Transferred 10 000 € to the account of Mr. U.
5.1.2016	Mr. Z withdrew 1 000 € from his account previously credited by Mr. Y and transferred 3 000 € on behalf of account of Mr. T. Mr. T put the fund in deposit. At this point, bank knows that Mr. T is an employee of company G.
8.1.2016	Mr. Z transferred again 3 000 € to Mr. T. Mr. T again put the fund in deposit.

Source: Own processing

[112]Examples of Suspicious Transactions. *www.sc.com* [online]. 2016 [cit. 2016-11-10]. Available from: https://www.sc.com.my/home/Anti-Money-laundering-and-anti-terrorism-financing/lists-of-suspicious-transactions/

From aforementioned web of transactions, following leading indicators that supports existence of suspicious transactions can be observed:

- Mr. X is a new client of the Bank X. Despite that, he carried out transactions in large amounts.
- Transactions were among connected parties.
- All in or out transactions happened consecutively either on same day or within a few days.
- Tax restitution should have been paid out to a company's account and not to a personnel account.

From the example can be concluded that detecting suspicious transactions requires a complex reflection, having powers of observation and ability to see connections. Furthermore, we can observe strong layering stage here in terms of depositing, transferring and withdrawing all over again. Entities obligated to report questionable transactions should use indicators to recognize situations that require scrutiny from AML/CTF perspective.

7.2 Shortages on the side of bank's Anti-money laundering policies

According to us, it is valuable when regulatory authorities disclose deficiencies detected in their countries. In this case, other authorities responsible for supervision can be aware of these practices and potentially draw from their experiences. Numbers of different shortcomings were observed in certain banks by regulatory authorities entitled with supervision of AML/CTF regime worldwide and thus we brought them together under the following categories:

- Correspondent banking.
- Wire transfers.
- High-risk customers and PEPs.
- Uncategorized shortages.

Correspondent banking

Correspondent banking relationships pose significant ML/TF risks since domestic bank executing the transaction must rely on the foreign bank proper identifying the client,

determining the real owners, and monitoring transactions for risks. The problem is that foreign bank's AML policy is adapted for its local country of operation. For this reason, we have considered important to elucidate several poor practices within correspondent banking relationships that were observed worldwide by regulatory bodies:

- Depending too much upon parent banks to perform monitoring of respondents without understanding it.
- Taking inadequate action when respondents do not provide satisfactory answers to reasonable questions concerning activities and movements on their account.
- Concentrating too much on reputational or business issues when deciding whether to exit relationships with respondents representing increased risk.
- No involvement of senior management in the approval process of new correspondent bank relationships or in the process of updating risk assessments of existing relationships.
- Failure or no attempt to assess new information collected throughout the relationship.
- Copying periodic assessment forms year after year without considering ML/TF alerts aroused since the last review.
- Relaying too much on the Wolfsberg AML questionnaire.[113]

Wire transfers

Due to the well-known connection between wire transfers and ML/TF, these transactions are put under a microscope. As methods of electronic funds transfers, wire transfers are core of AML/CTF practices and thus regulatory eyes are highly concentrated on them. Following common deficiencies are usually revealed:

- Not taking into account the FATF list of countries considered high-risk given their AML/CTF deficiencies. Certain banks simply decide to ignore high-risk indicators for various reasons. One of the reasons can be a many dealings with these customers or reluctance to carried out enhanced due diligence.
- Assessing sectors normally associated with increased corruption (pharmaceutical, extractive) as a low-risk just because these sectors are regulated. Important is that they are not regulated for AML purposes and this is what really matters.

[113]The Wolfsberg AML questionnaire can be found on this website: http://www.wolfsberg-principles.com/pdf/diligence/Wolfsberg-Anti-Money-Laundering-Questionnaire.pdf

- Allocating inadequately low-risk weightings for certain high-risk factors in order to avoid enhanced due diligence and wittingly not taking into account adverse information from wide range of sources.

High-risk clients and PEPs

Precise definition of PEP lacks but as we have defined it before, it is a person entrusted with a prominent public function. It goes without saying that PEPs present enhanced risk to be involved in bribery or corruption by the nature of their position and the power they hold. Normally, the continuing business relationship between the bank and the PEP is subject to stricter monitoring and examination than is the case with other, regular customers. Despite that, many insufficiencies are still being revealed what supports the inevitability to continue the rigid supervision regarding this type of clientele. Following shortages are common in case of PEPs:

- Changing the status of relationships from low-risk to high-risk shortly before the visit of regulatory authority.
- Permitting junior or otherwise inexperienced staff to play an integral part in on-going monitoring of high-risk clients and PEP.
- Copying information from the previous review without considering any kind of potentially increased risks.
- Failure to differentiate between source of funds and source of wealth.
- Unsatisfactory information on source of wealth that consequently results in failure to verify whether the wealth is linked to any kind of crime or not.
- Wittingly accepting the risk despite the potential of ML/TF simply due to a profitable business relationship.
- Failure to recognize and take into consideration credible allegations of criminal activity from reputable sources.
- Allowing personal accounts to be used for intentions not consistent with the expected activity on the account without any enquiry.
- Failure to give respective consideration to certain political connections which fall outside the definition of a PEP (wider family) which means that certain customers must still be treated as high-risk and subject to enhanced due diligence.
- Failure to perform enhanced due diligence regarding high-risk clientele and PEPs or having poor quality CDD.

- Failure to make adequate preparation and training to relevant personnel on how to comply with AML/CTF requirements for managing responsibly high-risk customers.

Uncategorized shortages:

- Failure to update customer risk assessment on a periodic basis even though KYC procedures are an on-going process that must be continuously reassessed.
- Inadequately trained personnel that is either unaware or not familiar with the risk assessment process and methodology.
- Scoring risk in a manner that it is nearly impossible or very unlikely for a certain client to be classified with high-risk status.
- Gathering CDD without an effort to assess them deeply.
- Not having adequate documentary evidence within CDD files to show why clients were rated high, medium or low-risk.
- Failure to conduct risk assessment at all or until shortly before the visit of regulatory authorities.

Since legitimizing illegally obtained money usually requires it to pass through one or more banks, it is of critical importance that AML strategies against it obligate banks to carry out certain checks and monitor transactions to ensure that accounts are not being misused for ML/TF. However, what is inevitable, is the process of examining whether banks conduct these requirements in precise and credible manner. Recently, there have been couple of high-profile Western bank (BNP Paribas, HSBC) scandals over ML what only confirms this urgency. In addition, it warns that ML sometimes comes directly from the management of banks. Furthermore, we are experiencing the trend that the regulation is becoming more and more complex and difficult. With the advent of increased terrorist attacks, some rapid and "panic" decision were made. The steps that banks and other financial services must take are nothing but costless. The question whether the costs of today's efforts to tackle ML/TF outweigh the benefits to society remains both unpleasant and unanswered. We hold the view that regulation concerning ML/TF must be as straightforward as it is possible. This guarantees its proper implementation and simplifies the consequent supervision. The problem is, if it is even possible with such a complex nature that ML/TF holds, not to mention growing possibilities that globalization, virtualization and financial integration is continuously creating.

Conclusion

This diploma thesis has aspired to demonstrate that laundered money moves like water that always finds its way through stones and hindrances. When it is unhindered and without control, it can have devastating consequences. Its *first aim*, to provide clear presentation of money laundering, has been achieved by careful choice of selected chapter that interlock conceptually and all are essential to our discussion. The *second objective*, to suggest the leading indicators, has been reached by recognition of vulnerabilities, such as low-quality Anti-money laundering regime or banking secrecy, and by realization of what yields the money laundering the most and then suggesting that it must be first eliminated so the consequent money laundering will not have chance to be born.

To document accurately the magnitude of its effect on real and financial sector is not feasible. However, since many traditional techniques are well-known, the adverse outcomes can be deduced. The major negative effect in terms of real sector certainly is diverting resources to less productive areas and creating unfair competition between legal and illegal businesses. This is caused by the fact that criminals do not think in rational economic way, on the contrary, their aim is to invest in sterile investments, such as real estate, that do not generate extra productivity. They set up business not to create a successful enterprise that can possibly invent something new or create additional working positions but to run it only for concealment of their illegal funds. Money laundering erodes financial system as well. Loss of critical trust of investors, enhanced costs in various areas, irrational impact on macroeconomic indicators and weakened role of the financial sector in economic growth is only a narrow selection of unfavourable effects.

We have also warned against growing potential of cyber laundering to call more attention to it. We hold the view that however the realization of its risks exists, the steps undertaken against it are still not sufficient. Even though we have evaluated positively the incorporation of online gambling in the fourth AML Directive, there are still loopholes that have not yet garnered enough attention on the legislation level. Fortunately, couple of months ago, European Commission has admitted the need of extending the latest Directive to virtual currencies. It goes without saying that this can be very important step towards eliminating this attractive laundering option.

Addressing money laundering through estimating the annual amount of laundered money still happens to be extremely difficult and inaccurate. It seems like we must get by with the fact that it is likely a tremendous amount and focus primarily on eliminating it. However, how do we know our countermeasures are strong and to maximum extent unbeatable? Since there is no possibility of comparing hard data, the only way to do so is by building a robust Anti-money laundering legislation and by recognizing possible leading indicators. Within this diploma thesis, we have divided them into two different groups as we have assumed that there are two fundamental ways to combat money laundering. *Firstly*, the reduction of money laundering can be achieved by decreasing criminal activity and thus eliminating it at the root, increasing transparency of financial secrecy havens and by recognizing high-risk jurisdiction and taking appropriate steps when dealing with them. *Secondly*, the mitigation of money laundering is likely to be reached by strong Anti-money laundering legislation and internal policies adopted by banks. Rigid and reliable internal systems within banks then lead to successful recognition of suspicious transactions.

In this diploma thesis, we have picked drug trafficking as leading indicator in regard with criminal activities. Drug money creates the biggest portion of illegal profit and thus drug trade and money laundering are in constant and mutual relationship. South America, with Colombia at the top, still produces coca at an alarming rate with even slight increase this year. This has not only terrible consequence on drug usage but the profit it generates must be somehow legitimized. This indicates that the demand for laundering is expected to rise. Similarly, Afghanistan continues to provide the rest of the world with heroin. Moreover, the Anti-money laundering measures in these countries still do not meet international standards what vastly hinders any improvement as well. More specifically, Afghanistan is still marked by FATF (Financial Act Task Force) as jurisdiction with Anti-money laundering strategic deficiencies. To continue, neighbouring Iran that plays a principle role in trafficking the heroin out of Afghanistan is still appearing on the FATF black list. Apparently, the combination of low Anti-money laundering habits together with widespread organized crime is fatal and extremely difficult to manage. We have proposed that regulatory authorities, such as UNODC (United Nations Office on Drugs and Crimes) and FATF, should continue to cooperate at maximum rate. In other words, as money laundering and drug trafficking is essential for one another, these institutions must adopt the same collaboration as well. Another indicator that we have considered reasonable is financial secrecy. Secrecy jurisdictions are much less engaged in sharing information with other nations and less

compliant regarding money laundering. Reluctance in information exchange together with lack of transparency makes them a perfect destination for routing illegal financial flows and obscuring criminal acts. As we could see, important in this matter is that not only traditionally perceived offshore centres are marked as secrecy jurisdictions but also countries such as USA, Switzerland, Singapore or Germany attack the top spots and deserve attention. In connection with this, we hold the view that the new project of automatic exchange of information might largely contribute to alleviate the negative outcomes of financial secrecy. However, its true results will be seen in the future.

In the last part of this diploma thesis, we have demonstrated basic Anti-money laundering measures adopted by selected jurisdiction, the Czech Republic. The country's location within Europe leaves it very vulnerable to any type of money laundering. Although the aim of this part was not to assess the Czech Anti-money laundering system but rather offer a general illustration of certain AML measures, we believe Czech Republic disposes of sufficient legislation with regular amendments. To be specific, we have evaluated positively measures incorporated against virtual currencies and the steps undertaken against online gambling industry that were underestimated for long time.

The significance of sophisticated internal systems within banks has been highlighted as another type of defence against money laundering. In most cases, money laundering cannot happen without banks being involved and therefore their participation is essential. Having said that, we have witnessed several shocking cases where international banks were part of money laundering or breaking sanctions. This destroys any attempts to solve the problem of money laundering by strong policies and hiring qualified and trained staff. Due to this, we are of the opinion that regulatory authorities must continue deep assessment of bank's procedures in this matter. In addition, we believe that cooperation between regulatory authorities in terms of disclosing deficiencies that were found out can lead to great results.

Solving the issue of money laundering is a long-term international goal. The FATF can be considered a global regulator in certain sense, but it has no power to sanction. We hold the strong conviction that successful war against money laundering will never be won by

fighting it by each jurisdiction individually. As we could see, it is a cross border problem that requests consistent and continuous global approach.

List of boxes, graphs, pictures, tables and appendix figures

References

Books:

1. BANKS, James. *Online gambling and crime: causes, controls and controversies*. Farnham: Ashgate, 2014. ISBN 978-1-4724-1449-6.
2. MASCIANDARO, Donato. TAKÁTS, Elöd. UNGER, Brigitte. *Black Finance: The Economics of Money Laundering.* Cheltenham (UK): Edward Elgar, 2007. ISBN 10-1782543473

E-books:

1. BURKE, Jason. *Al-Qaeda: the true story of radical Islam*. [e-book]. 3rd ed. London: Penguin, 2007. ISBN 9780141031361. Available from: https://books.google.cz/books/about/Al_Qaeda.html?id=-_FJFFrit8AC&redir_esc=y
2. FOREST, James J. F. *Essentials of counterterrorism*. [e-book]. Santa Barbara, California: Praeger, an imprint of ABC-CLIO, LLC, 2015. ISBN 9781440834707. Available from: https://books.google.cz/books/about/Essentials_of_Counterterrorism.html?id=fcihCgAAQBAJ&redir_esc=y
3. HINTERSEER, Kris. *Criminal finance: the political economy of money laundering in a comparative legal context*. [e-book] Boston, Mass.: Kluwer Law International, 2002. ISBN 9041198644. Available from: https://books.google.cz/books/about/Criminal_Finance_The_Political_Economy_o.html?id=Cx3x4EijpXsC&redir_esc=y
4. RYDER, Nicholas. *The financial war on terrorism: a review of counter-terrorist financing strategies since 2001*. [e-book] Abingdon, Oxon: Routledge, 2015. Law of financial crime. ISBN 0415640385. Available from: https://books.google.cz/books/about/The_Financial_War_on_Terrorism.html?id=ZM-rMQEACAAJ&redir_esc=y
5. RICHARDS, James R. *Transnational criminal organizations, cybercrime, and money laundering: a handbook for law enforcement officers, auditors, and financial investigators*. [e-book]. Boca Raton, FL: CRC press, c1999. ISBN 0849328063. Available from: https://books.google.cz/books/about/Transnational_Criminal_Organizations_Cyb.html?id=RmGi5zDus7gC&redir_esc=y
6. SCHOTT, Paul. *Reference guide to Anti-Money laundering and combating the financing of terrorism*. [e-book] .2nd ed. Washington, D.C.: World Bank, c2006. ISBN 0-8213-6513-4. Available from: https://books.google.cz/books/about/Reference_Guide_to_Anti_money_Laundering.html?id=qRJlAXxAOCwC&redir_esc=y
7. SPARKES, Peter. *European land law*. [e-book]. Portland, Or.: Hart, 2007. ISBN 1841137588. Available from: https://books.google.cz/books/about/European_Land_Law.html?id=3e7bBAAAQBAJ&redir_esc=y
8. WILLIAM H. BYRNES, ROBERT J. MUNRO., William H. Byrnes, Robert J. Munro. *Money laundering, asset forfeiture and recovery, and compliance: a global guide*. [e-book]. 2011. ISBN 9780327170846. Available from:

https://books.google.cz/books/about/Money_Laundering_Asset_Forfeiture_and_Re.html?id=cVLUdo4JQv4C&redir_esc=y

Internet sources:

1. 10 Biggest Heroin Trafficking Countries In The World. *www.therichest.com* [online]. 2014 [cit. 2016-09-21]. Available from: http://www.therichest.com/rich-list/the-biggest/the-10-hottest-countries-in-heroin-trafficking/
2. AEOI: Status of commitments. *www.oecd.org* [online]. 2016 [cit. 2016-09-10]. Available from: http://www.oecd.org/tax/transparency/AEOI-commitments.pdf
3. A simple guide to safely and effectively tumbling bitcoins. *www.darknetmarkets.org* [online]. 2015;; [cit. 2016-08-30]. Available from: https://darknetmarkets.org/a-simple-guide-to-safely-and-effectively-mixing-bitcoins
4. AML global alignment: Two steps forward, one step back. *Www.pwc.com* [online]. 2015 [cit. 2016-09-02]. Available from: http://www.pwc.com/us/en/financial-services/regulatory-services/publications/assets/aml-global-alignment.pdf
5. Bank secrecy. *www.swiss-privacy.com* [online]. [cit. 2016-09-11]. Available from: https://www.swiss-privacy.com/bank-secrecy.html
6. Bitcoin tumbler: The business of covering tracks in the world of cryptocurrency laundering. *www.ibtimes.co.uk* [online]. 2015 [cit. 2016-08-30]. Available from: http://www.ibtimes.co.uk/bitcoin-tumbler-business-covering-tracks-world-cryptocurrency-laundering-1487480
7. BRYANS, Danton. Bitcoin and Money Laundering: Mining for an Effective Solution. In: *Indiana Law Journal*[online]. p. 33 [cit. 2016-08-25]. Available from: http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=11100&context=ilj
8. Computer Emergency Response Team - Laboratoire d'Expertise en Sécurité Informatique (2006). Online Gaming Cybercrime: CERT-LEXSI'S White Paper, July 2006.
9. Colombia. *www.Anti-Moneylaundering.org* [online]. 2014 [cit. 2016-10-06]. Available from: http://www.Anti-Moneylaundering.org/southamerica/Colombia.aspx
10. Colombia's Discount Currency Exchanges Are Funneling Drug Money. *www.bloomberg.com* [online]. 2016 [cit. 2016-10-07]. Available from: http://www.bloomberg.com/news/articles/2016-01-28/cocaine-s-unbroken-grip-on-currency-market-trading-in-colombia/Colombia.aspx
11. Countering Money Laundering and the Financing of Terrorism. *Asian Development Bank* [online]. 2003 [cit. 2016-08-14]. Available from: https://www.unodc.org/tldb/pdf/Asian-bank-guide.pdf
12. Criminalizing the laundering of proceeds of trafficking in persons. *Https://www.unodc.org/* [online]. [cit. 2016-08-02]. Available from: https://www.unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_3-5.pdf
13. Customer Identification Program (CIP). *www.advisoryhq.com* [online]. 2016 [cit. 2016-11-01]. Available from: http://www.advisoryhq.com/articles/developing-a-well-defined-customer-identification-program-cip/
14. Dirty Money in Afghanistan: How Kabul is Cleaning Up the Illicit Economy. *www.foreignaffairs.com*[online]. 2016 [cit. 2016-09-23]. Available from: https://www.foreignaffairs.com/articles/afghanistan/2016-09-07/dirty-money-afghanistan

15. Examples of Suspicious Transactions. *www.sc.com* [online]. 2016 [cit. 2016-11-10]. Available from: https://www.sc.com.my/home/Anti-Money-laundering-and-anti-terrorism-financing/lists-of-suspicious-transactions/
16. E-money. *www.ec.europa.eu* [online]. 2015 [cit. 2016-08-21]. Available from: http://ec.europa.eu/finance/payments/emoney/index_en.htm
17. *FATF* [online]. [cit. 2016-09-01]. Available from: http://www.fatf-gafi.org
18. FAÚ. *www.mfcr.cz* [online]. 2016 [cit. 2016-11-03]. Available from: http://www.mfcr.cz/cs/zahranicni-sektor/ochrana-financnich-zajmu/boj-proti-prani-penez-a-financovani-tero/zakladni-informace
19. FIEDLER, Ingo. *Online Gambling as a Game Changer to Money Laundering?* [online]. In: . WiSo-Fakultät : Universität Hamburg, 2013, p. 14 [cit. 2016-08-23]. Available from: https://www.wiso.uni-hamburg.de/fileadmin/bwl/rechtderwirtschaft/institut/Ingo_Fiedler/Online_Gambling_as_a_Game_Changer_to_Money_Laundering_01.pdf
20. FILIPKOWSKI, Wojciech. Cyber Laundering: An Analysis of Typology and Technique In: *International Journal of Criminal Justice Sciences* [online]. [cit. 2016-08-20]. Available from: https://www.researchgate.net/publication/222099776_Cyber_Laundering_An_Analysis_of_Typology_and_Techniques
21. Financial Secrecy Index 2015 reveals improving global financial transparency, but USA threatens progress. *Www.taxjustice.net* [online]. [cit. 2016-09-16]. Available from: http://www.taxjustice.net/wp-content/uploads/2013/04/FSI-2015-Presser.pdf
22. Financial Secrecy Index. *www.financialsecrecyindex.com* [online]. [cit. 2016-09-18]. Available from: http://www.financialsecrecyindex.com
23. Financial System Abuse, Financial Crime and Money Laundering. *IMF* [online]. 2001 [cit. 2016-08-12]. Available from: https://www.imf.org/external/np/ml/2001/eng/021201.pdf
24. For European banks, US assurances on Iran come with asterisks. *www.reuters.com* [online]. 2016 [cit. 2016-09-03]. Available from: http://www.reuters.com/article/us-usa-sanctions-iran-idUSKCN0Y92WI
25. FREEMAN, Michael. The sources of terrorist financing: theory and typology. In: *Calhoun: The NPS Institutional Archive* [online]. 2011 [cit. 2016-08-30]. Available from: http://calhoun.nps.edu/bitstream/handle/10945/47781/Freeman-The-Sources-of-Terrorist-Financing_2010.pdf?sequence=1
26. *Gray Money* [online]. [cit. 2016-07-29]. Available from: http://financial-dictionary.thefreedictionary.com/Gray+Money
27. HE, Dong a Karl HABERMEIER. Virtual Currencies and Beyond: Initial Considerations. In: *IMF* [online]. p. 42 [cit. 2016-08-29]. Available from: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf
28. History of the European Union Anti-Money Laundering and Financing of Terrorism Directives. *www.Anti-Moneylaundering.org* [online]. 2015 [cit. 2016-09-02]. Available from: http://www.Anti-Moneylaundering.org/Europe.aspx
29. How to Fight Prepaid Card Fraud. *www.bankinfosecurity.com* [online]. 2014 [cit. 2016-08-26]. Available from: http://www.bankinfosecurity.com/interviews/how-to-mitigate-prepaid-card-fraud-i-2149
30. HSBC to pay $1.9 billion US fine in money-laundering case. *www.reuters.com* [online]. 2012 [cit. 2016-10-07]. Available from: http://www.reuters.com/article/us-hsbc-probe-idUSBRE8BA05M20121211

31. Illicit trafficking in narcotic drugs and money laundering. *www.menafatf.org* [online]. 2011 [cit. 2016-09-21]. Available from: http://www.menafatf.org/images/UploadFiles/Illicit_Trafficking_and_ML_Eng.pdf
32. Internet Access Is Now A Basic Human Right. *www.gizmodo.com* [online]. 2016 [cit. 2016-08-25]. Available from: http://gizmodo.com/Internet-access-is-now-a-basic-human-right-1783081865
33. INTERNET USAGE STATISTICS The Internet Big Picture. *www.Internetworldstats.com* [online]. 2016 [cit. 2016-08-25]. Available from: http://www.Internetworldstats.com/stats.htm
34. IPAS, Roxana. Money laundering through offshore areas. In: *Annals of the University of Petroşani, Economics,* [online]. 2009 [cit. 2016-09-10]. Available from: http://upet.ro/annals/economics/pdf/2009/20090209.pdf
35. Jackpot! Money laundering through online gambling. *www.mcafee.com* [online]. 2014 [cit. 2016-08-25]. Available from: http://www.mcafee.com/es/resources/white-papers/wp-jackpot-money-laundering-gambling.pdf
36. JOST, Patrick. The Hawala alternative remittance system and its role in ML. In: *United States Department of the Treasury* [online]. [cit. 2016-08-08]. Available from: https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/FinCEN-HAWALA-rpt.pdf
37. KEHOE, Mark. *The threat of Money Laundering* [online]. In: . 1996 [cit. 2016-08-14]. Available from: http://econserv2.bess.tcd.ie/SER/1996/mkehoe.htm
38. KYC/AML/CTF/International Sanctions Program. *www.unicredit.ro* [online]. 2016 [cit. 2016-11-03]. Available from: https://www.unicredit.ro/content/dam/cee2020-pws-ro/DocumentePDF/Banci-corespondente/KYC_AML%20Policy%20UCT.PDF
39. KUMAR, Vandana. Money Laundering: Concept, Significance and its Impact. *In: European Journal of Business and Management* [online]. 2012 [cit. 2016-08-14]. ISSN 2222-2839 Available from: http://www.iiste.org/Journals/index.php/EJBM/article/view/1040/960
40. LIPPERT, O. a M. WALKER. *The underground economy: Global evidence of its size and impact.* [online]. In: . Vancouver, B.C., Canada: The Fraser Institute, 1997, s. 350 [cit. 2016-07-29]. Available from: www.fraserinstitute.org/sites/default/files/UndergroundEconomy.pdf
41. London property market turned into money laundering safe haven by inadequate supervision. *www.independent.co.uk* [online]. 2016 [cit. 2016-08-14]. Available from: http://www.independent.co.uk/news/business/news/london-property-market-real-estate-money-laundering-overseas-foreign-buyers-mps-a7138176.html
42. *Money Laundering* [online]. [cit. 2016-07-29]. Available from: http://www.investopedia.com/terms/m/moneylaundering.asp
43. *Money Laundering in the EU: Methods and Stages of Money Laundering* [online]. [cit. 2016-07-30]. Available from: http://people.exeter.ac.uk/watupman/undergrad/ron/methods%20and%20stages.htm
44. *Money Laundering: A three-stage process* [online]. [cit. 2016-07-30]. Available from: https://www.moneylaundering.ca/public/law/3_stages_ML.php
45. Money-Laundering and Globalization. *United Nations office on Drugs and Crime* [online]. [cit. 2016-08-11]. Available from: https://www.unodc.org/unodc/en/money-laundering/globalization.html
46. Money laundering through real estate. *Australian Government* [online]. [cit. 2016-08-14]. Available from: https://www.innanrikisraduneyti.is/media/peningathvaetti/MoneyLaunderingThroughRealEstate.pdf

47. MoneyWeb - Uživatelský manuál pro povinné subjekty. *Http://ca.moneyweb.cz* [online]. 2008 [cit. 2016-11-20]. Available from: http://ca.moneyweb.cz/mwlite/MoneyWeb_Lite-user_manu
48. Monitoreo de territorios afectados por cultivos ilícitos 2015.*www.unodc.org* [online]. 2016 [cit. 2016-10-05]. Available from: http://www.unodc.org/documents/crop-monitoring/Colombia/Monitoreo_Cultivos_ilicitos_2015.pdf
49. Office of Foreign Assets Control (OFAC). *www.treasury.gov* [online]. 2015 [cit. 2016-09-02]. Available from: https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx
50. Offshore Financial Centers. *www.imf.org* [online]. [cit. 2016-09-10]. Available from: https://www.imf.org/external/np/mae/oshore/2000/eng/back.htm#II_A
51. *Prepaid card, mobile payments and Internet-based payment services* [online]. The FATF, 2013 [cit. 2016-08-22]. Available from: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf
52. Public Statement - 24 June 2016. *www.fatf-gafi.org* [online]. [cit. 2016-09-20]. Available from: http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-june-2016.html
53. QUIRK, Peter. Money Laundering: Muddying the Macroeconomy. In: *IMF* [online]. Washington, 1997 [cit. 2016-08-14]. Available from: https://www.imf.org/external/pubs/ft/fandd/1997/03/pdf/quirk.pdf
54. RICKMAN, Andy. Cyberlaundering: The Risks, the Responses. In: *Law Faculty Scholarly Articles* [online]. [cit. 2016-08-22]. Available from: http://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1326&context=law_facpub
55. Sanctions. *www.un.org* [online]. 2016 [cit. 2016-09-01]. Available from: https://www.un.org/sc/suborg/en/sanctions/information
56. Sanctions policy. www.eeas.europa.eu [online]. 2016 [cit. 2016-09-01]. Available from: https://eeas.europa.eu/topics/sanctions-policy/423/sanctions-policy_en
57. SCHNEIDER, Friedrich. Shadow Economies All over the World. In: *www.worldbank.org* [online]. 2010 [cit. 2016-07-28]. Available from: https://openknowledge.worldbank.org/bitstream/handle/10986/3928/WPS5356.pdf?sequence=1
58. SCHNEIDER, Friedrich. The Shadow Economy and Work in the Shadow: What Do We (Not) Know? In: *www.iza.org/en/webcontent/index_html* [online]. 2012 [cit. 2016-07-29]. Available from: http://ftp.iza.org/dp6423.pdf
59. SIENKIEWICZ, Stanley. *Prepaid Cards: Vulnerable to Money Laundering?* [online]. In: 2007, s. 22 [cit. 2016-08-23].
60. Simon's Guide to Online Gambling Legal Status and Laws. *www.explainbetter.wordpress.com* [online]. 2016 [cit. 2016-08-25]. Available from: https://simonsblogpark.com/onlinegambling/simons-guide-online-gambling-legal-status-laws/
61. Standard for Automatic Exchange of Financial Account Information. *www.oecd.org* [online]. [cit. 2016-09-11]. Available from: https://www.oecd.org/ctp/exchange-of-tax-information/automatic-exchange-financial-account-information-common-reporting-standard.pdf
62. STRAUSS, Kilian. How can we effectively combat the use of the Internet for money laundering? In: *Kilian Strauss* [online]. [cit. 2016-08-20]. Available from: http://www.academia.edu/1369342/Cyber laundering_-_How_can_we_combat_money_laundering_over_the_Internet

63. Tanzi, Vito. 1999. *Uses and Abuses of the Estimates of The Underground Economy.* [online]. 1999 [cit. 2016-11-03]. Economic Journal 109:338-47. Available from: https://www.jstor.org/stable/2566007?seq=1#page_scan_tab_contents
64. Terrorism. *www.en.oxforddictionaries.com* [online]. 2014 [cit. 2016-08-26]. Available from: http://www.oxforddictionaries.com/definition/english/terrorism
65. Terrorist financing: definition and methods. *www.fidis.net* [online]. [cit. 2016-08-30]. Available from: http://www.fidis.net/resources/fidis-deliverables/identity-of-identity/int-d2200/doc/27/
66. Terrorist financing. *www.fatf-gafi.org* [online]. 2008 [cit. 2016-08-26]. Available from: http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf
67. The Eighth Annual Prepaid Forecast. *www.mercatoradvisorygroup.com* [online]. 2011 [cit. 2016-08-26]. Available from: https://www.mercatoradvisorygroup.com/Reports/The-Eighth-Annual-Prepaid-Forecast/
68. The Fourth EU Anti Money Laundering Directive. *www2.deloitte.com* [online]. [cit. 2016-09-02]. Available from: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/investmentmanagement/ie_2015_The_Fourth_EU_Anti_Money_Lawndering_Directive_Deloitte_Ireland.pdf
69. The Fourth EU Anti Money Laundering Directive European Commission Update. *www2.deloitte.com* [online]. 2016 [cit. 2016-09-02]. Available from: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/IE_2016_fourth_EU_AML_Directive.pdf
70. The role of financial markets for economic growth. *ECB* [online]. [cit. 2016-08-11]. Available from: https://www.ecb.europa.eu/press/key/date/2001/html/sp010531.en.html
71. The role of Hawala in ML and TF. *FATF* [online]. [cit. 2016-08-08]. Available from: https://www.imolin.org/pdf/imolin/Role-of-hawala-and-similar-in-ml-tf-1.pdf
72. The Secrets of Online Money Laundering. *www.technologyreview.com* [online]. 2013 [cit. 2016-08-15]. Available from: https://www.technologyreview.com/s/520501/the-secrets-of-online-money-laundering/
73. The third EU directive on money Laundering and terrorist Financing. In: VYHNÁLIK, Ján. *NBS* [online].[cit. 2016-09-02]. Available from: http://www.nbs.sk/_img/Documents/BIATEC/BIA09_05/11_15.pdf
74. THOMPSON, Edwina. The nexus of drug trafficking and Hawala in Afghanistan. In: *Http://www.worldbank.org* [online]. [cit. 2016-08-08]. Available from: http://siteresources.worldbank.org/SOUTHASIAEXT/Resources/Publications/448813-1164651372704/UNDC_Ch6.pdf
75. THONY, Jean-François. In: *IMF* [online]. [cit. 2016-08-30]. Available from: http://www.imf.org/external/np/leg/sem/2002/cdmfl/eng/thony.pdfttp://www.imf.org/external/np/leg/sem/2002/cdmfl/eng/thony.pdf
76. The Wolfsberg Group. *www.wolfsberg-principles* [online]. 2016 [cit. 2016-09-04]. Available from: http://www.wolfsberg-principles.com/index.htm
77. Using Bitcoin Casinos To Launder Bitcoin. *www.bitcoinbabeau.wordpress.com* [online]. 2016 [cit. 2016-08-30]. Available from: https://bitcoinbabeau.wordpress.com/2016/04/13/using-bitcoin-casinos-to-launder-bitcoin/
78. Vancouver housing market 'vulnerable' to money laundering. *Www.theglobeandmail.com* [online]. 2016 [cit. 2016-08-15]. Available

from: http://www.theglobeandmail.com/news/national/vancouver-housing-market-vulnerable-to-money-laundering/article29285770/
79. Virtual currencies. *The FATF* [online]. 2015 [cit. 2016-08-25]. Available from: http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf
80. Virtual Money Laundering and Fraud. Www.bankinfosecurity.com [online]. 2008 [cit. 2016-08-25]. Available from: http://www.bankinfosecurity.com/virtual-money-laundering-fraud-a-809
81. Výroční zpráva FAÚ 2015. In: *www.mfcr.cz* [online]. 2015 [cit. 2016-11-18]. Available from: http://www.mfcr.cz/cs/zahranicni-sektor/ochrana-financnich-zajmu/boj-proti-prani-penez-a-financovani-tero/vysledky-cinnosti-financniho-analytickeh/2015/zprava-o-cinnosti-financniho-analytickeh-24287
82. *What is prepaid card?* [online]. [cit. 2016-08-22]. Available from: http://www.mastercard.com/hk/consumer/prepaid-card.html
83. World Drug Report. *www.unodc.org* [online]. 2016 [cit. 2016-09-21]. Available from: https://www.unodc.org/doc/wdr2016/WORLD_DRUG_REPORT_2016_web.pdf
84. What is Hawala Money? Explained. *Www.explainbetter.wordpress.com* [online]. 2015 [cit. 2016-08-08]. Available from: https://explainbetter.wordpress.com/2015/02/03/what-is-hawala-money-explained/

Legislation:

1. Act No. 253/2008 Coll. of 19 October, 2016 on selected measures against legitimisation of proceeds of crime and financing of terrorism. Available from: http://www.epravo.cz/_dataPublic/sbirky/2016/sb0147-2016.pdf
2. No. 281/2008 Coll. of 25 June 2014 on certain requirements for the system of internal principles, procedures and control measures against money laundering and terrorist financing. Available from: http://www.epravo.cz/top/zakony/sbirka-zakonu/vyhlaska-ze-dne-25-cervna-2014-kterou-se-meni-vyhlaska-c-2812008-sb-o-nekterych-pozadavcich-na-system-vnitrnich-zasad-postupu-a-kontrolnich-opatreni-proti-legalizaci-vynosu-z-trestne-cinnosti-a-financovani-terorismu-20119.html
3. EU Directive 2015/849 of the European parliament and of the council of 20 May 2015 on the prevention of the use of the financial system for the purposes of ML/TF. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849

Appendix

Appendix figure 1: AEOI: status of commitments

Countries undertaking first exchange by 2017
Argentina, Anguilla, Belgium, Barbados, Bermuda, Bulgaria, British Virgin Islands, Cayman Islands, Croatia, Colombia, Cyprus, Curacao, Czech Republic, Denmark, Estonia, Finland, Faroe Islands, France, Germany, Gibraltar, Greece, Guernsey, Hungary, India, Iceland, Ireland, Italy, Isle of Man, Jersey, Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Montserrat, Malta, Mexico, Netherlands, Norway, Niue, Portugal, Poland, Romania, Seychelles, San Marino, Slovenia, Slovak Republic, South Africa, Sweden, Spain, Trinidad and Tobago, UK
Countries undertaking first exchange by 2018
Albania, Antigua and Barbuda, Andorra, Australia, Aruba, Austria, The Bahamas, Bahrain, Brazil, Belize, Brunei Darussalam, Canada, China, Chile, Cook Islands, Costa Rica, Dominica, Ghana, Grenada, Hong Kong, Indonesia, Japan, Israel, Kuwait, Marshall Islands, Lebanon, Macao (China), Malaysia, Monaco, Mauritius, Nauru, New Zealand, Qatar, Panama, Russia, Saint Lucia, Samoa, Saint Vincent and the Grenadines, Singapore, Saudi Arabia, Switzerland, Sint Maarten, Turkey, UAE, Uruguay, Vanuatu

Source: OECD (2)

Appendix figure 2: Sections under which the FATF recommendations are included

AML/CTF policies and coordination.
ML and confiscation.
TF
Preventive measures.
Transparency and beneficial ownership of legal persons and arrangements.
Powers and responsibilities of competent authorities and other institutional measures.
International cooperation.

Source: the FATF (18)

Appendix figure 3: The Wolfsberg standards

The Wolfsberg CB Principles
The Wolfsberg Group MIPS Paper
The Wolfsberg Private Banking Principles
The Wolfsberg Guidance on Prepaid and Stored Value Cards
The Wolfsberg Anti-Corruption Guidance
The statement on the publication of the Wolfsberg Anti-Corruption Guidance
The Wolfsberg Trade Finance Principles
The Wolfsberg Monitoring Screening Searching Paper
The Wolfsberg AML Guidance on Credit/Charge Card Issuing and Merchant Acquiring Activities
The Wolfsberg Group, Clearing House Statement on Payment Message Standards
The Wolfsberg Group, Notification for Correspondent Bank Customers
The Wolfsberg Statement- Guidance on a Risk-based Approach for Managing ML Risks
The Wolfsberg statement- AML Guidance for Mutual Funds and Other Pooled Investment Vehicles
The Wolfsberg Statement on The Suppression of the Financing of Terrorism

Source: Wolfsberg group (76)