NOVA SCHOOL OF LAW

NOVA IMS
Information
Management
School

MATHEUS MARTINEZ JIMENEZ

UNWANTED ENTAILMENTS OF THE CURRENT EU AML/CFT REGIME

Dissertation to obtain a Master's Degree in Law,
in the specialty of Law and Financial Markets

Supervisor:
Dr. Lúcio Tomé Feteira, Professor of the NOVA School of Law

September 2022

NEW UNIVERSITY OF LISBON

NOVA SCHOOL OF LAW AND NOVA INFORMATION MANAGEMENT SCHOOL

MASTER'S IN LAW AND FINANCIAL MARKETS

MATHEUS MARTINEZ JIMENEZ

UNWANTED ENTAILMENTS OF THE CURRENT EU AML/CFT REGIME

Dissertation to obtain a Master's Degree in Law,
in the specialty of Law and Financial Markets

Supervisor:
Dr. Lúcio Tomé Feteira, Professor of the NOVA School of Law

September 2022

ANTI-PLAGIARISM STATEMENT

I declare, on my honour, that the work I present is original and that all my citations are correctly identified. I am aware that the use of unidentified elements from others constitutes a serious ethical and disciplinary fault.

MATHEUS MARTINEZ JIMENEZ

Lisbon, September 15th 2022

ACKNOWLEDGMENTS

To all my family and friends who helped me throughout this journey, to all my professors and tutors who enlightened me, an honest appreciation.

"We have always known that heedless self interest was bad morals, we now know that it is bad economics."
— Franklin Delano Roosevelt

MODE OF CITATION AND ADOPTION OF STANDARDS

The standard adopted for citation, footnotes, bibliography and others is NP 405.1 and 405-4.

NUMBER OF CHARACTERS

The body of this dissertation (including spaces and footnotes) contains 112,238 characters between the Introduction and the Conclusion, not including the initial part and the bibliography.

LIST OF ACRONYMS AND ABBREVIATIONS

EU – European Union

ECHR – European Court of Human Rights

AML – Anti money laundering

CFT – Counter finance of terrorism

ML – Money laundering

AMLD – Anti money laudering directive

PEPs – Politically exposed person

NGO – Nor for profit organizations

FATF – Financial action task force

FIU – Financial Intelligence Units

EDD – Enhanced due diligence

SPP – Special due diligence

FCA – Financial conduct authority

GDPR - General Data Protection Regulation

HCI – Human-computer interaction

AI – Artificial intelligence

RESUMO

A presente tese visa investigar, de forma pragmática, a batalha contra o financiamento do terrorismo e o branqueamento de capitais no contexto do quadro europeu existente, bem como algumas das suas repercussões indesejadas. Para atingir esse objetivo, foi dada uma elucidação abrangente de todo o processo. A investigação, a acusação e a punição de todas as formas de enriquecimento ilícito estão atualmente em voga, bem como, sem dúvida, o financiamento do terrorismo. A monitorização das transações recebeu uma ênfase especial porque é a génese de alertas automatizados de atividades invulgares, dentro de um esquema complexo de relatórios. Foi utilizada uma abordagem técnica do instrumento, especialmente para ilustrar os custos de contingência e prudenciais esperados das instituições financeiras. Os determinantes dos fatores de risco num dado contexto também estavam sob escrutínio, bem como a necessidade de transparência num dado sistema. A tese também elucidou a incongruência de questões de aparente interesse público, nomeadamente a prevenção do branqueamento de capitais e financiamento do terrorismo e as suas reflexões negativas na proteção do consumidor e na integração financeira.

Palavras-chave: Branqueamento de capitais, financiamento do terrorismo, sistemas de monitorização de transações, finanças empresariais, transparência, integração financeira, gestão de risco.

ABSTRACT

The current thesis aimed to pragmatically investigate the battle against terrorism financing and money laundering in the context of the existing European framework, as well as some of its unintended repercussions. To achieve that goal, a comprehensive elucidation of the whole process was given. Investigation, prosecution, and punishment of all forms of illicit enrichment are currently in vogue., as well as, undoubtedly, the financing of terrorism. Transaction monitoring was given a special emphasis because it is the genesis of automated alerts of unusual activities, within a complex reporting scheme. A technical approach of the tool was utilized, especially to illustrate the contingency and prudential costs expected of financial institutions. The determinants of risk factors in given context were also under scrutiny, so was the need for transparency in given system. The thesis also elucidated the incongruity of two seemly public interest matters ML-FT prevention and its negative reflections in consumer protection and financial integration.

Key-Words: Money laundering, terrorism financing, transaction monitoring systems, risk factors, transparency, financial integration, risk-assessment

GENERAL INDEX

INTRODUCTION

The present research aims to pragmatically examine the battle against terrorism financing and money laundering in the context of the existing European framework, as well as some of its unintended repercussions. To achieve that goal, a comprehensive elucidation of the whole process was given.

The growth of money laundering and terrorist funding, coupled with tax evasion and state austerity programmes, has pushed the fight against money laundering and financial crime onto the political agenda of the European Union (EU). All the more reason for anti-money laundering policymakers in the EU to preserve the Union's linked financial markets by prosecuting all activities that generate illegal wealth. The current trend is to investigate, prosecute, and punish all forms of illicit enrichment (corruption, tax evasion, private corruption, insider trading, misuse of money, market abuse, counterfeiting, and piracy), including criminal infiltration of financial institutions and businesses and for obvious reasons, the financing of terrorism (Ioannides, 2014, p. 19).

Currently there are five phases of money laundering prevention and control: genesis of automated alerts of unusual financial activities; internal processing of the findings of suspicion by financial institutions; submission of Suspicious Activity Reports as disclosures of alleged offences to financial intelligence units (triggering the investigation of the financial affairs of suspects); confidential and compatible with the European court of human rights (ECHR) financial investigations of suspects; and prosecution of suspects for money laundering, the bringing of the indictment for the offences, and trial (Ioannides, 2014, p. 3).

Transaction monitoring was given a special emphasis because it constitutes itself as the first phase – genesis of automated alerts of unusual activities. As will be shown, the risk-based strategy imposed by the 4th AMLD broadens the playing field, as there are many permutations of the methodology and uncountable judgments to be taken (Chau *et al.*, 2020, p. 37). A human analyst will ultimately examine the generated warnings to evaluate whether the technology appropriately identified the condition. This might be the compliance analyst of the financial institution, his or her colleague or boss, an internal audit team, a regulatory watchdog audit team, or the FIU analysts to whom really suspicious incidents are reported (Chau *et al.*, 2020, p. 29).

Furthermore, the said risk-based requires banks to evaluate their customers based on factors such as sector/occupation risk, nationality risk and jurisdictional/political risk. Be there as it may, there are no commonly accepted methods for assessing such risk factors, banks are enforced to develop their own measures of risk.

In addition to legal and ethical concerns, regulatory compliance imposes on banks stricter prudential criteria that incur greater expenses. Particularly in environments where banks are under increasing pressure to focus on their core business or are undergoing reorganization, expansion, or high staff turnover, executives are concerned about having the personnel and resources necessary to meet increasingly onerous compliance requirements. This broad drop in risk appetite on the side of banks may result in decisions to terminate client relationships, even with long-standing, problem-free, and ostensibly low-risk consumers and enterprises (Artingstall *et al.*, 2016, p. 16).

De-risking is a broad phenomena in which an organization attempts to decrease its exposure to risk by discontinuing operations en masse rather than on an individual basis. This could be the case for some alleged high-risk[1] consumers such as politically-exposed-persons (PEPs), non-for-profit organizations and nationals from poorly developed countries. If banks are to discontinue relations with these types of clients solemnly based on overbearing compliance costs, we could be looking at a reduction in the transparency of financial flows, since whole sorts of costumers must resource to other methods of banking.

Nonetheless, in October 2014, the Financial Action Task Force (FATF, 2014) addressed the issue of wholesale de-risking, arguing that risks should be assessed on a "case-by-case basis.". At the end of the day, however, it is a commercial decision of the bank. Even if that's not the case with all banks, the instance of "high-risk costumer" poses as an example of the general rule that, if a client is determined to be outside the bank's risk appetite, it will be very difficult to demonstrate that they actually represent a reduced risk; in other words, it is an attempt to demonstrate the opposite. It seems

[1] Based on FATF recommendations.

necessary to move further down the path of devolving responsibility for risk assessment to the national and institutional level, replacing the requirement for enhanced due diligence in specific cases with a requirement for due diligence directly correlated with the level of risk identified by the relevant risk assessment (Sciurba, 2018).

A holistic approach of the risk factors is required, as uncountable judgments are to be taken. As an alert is generated, in case of suspicion, the financial operator must not only inquire about the identity and basic risk factors of the parties involved, but also about the economic motivations for the transaction. Oftentimes, identification and basic risk assessment, such as a risk scorecard are insufficient; only when financial operators are required to match their information on transactions with data on the client and sometimes even their knowledge of the client's performance over a period of time can suspicious structures become evident. Without this requirement, it will be a matter of chance whether a transaction is actually deemed suspicious (Pieth, 1998).

With that in mind, the following questions were raised: What are the fundamental concepts that the current EU reporting system entails? What is the main tool utilized for combating the issue? What is the apparent conflict of two seemly public interest matters ML-FT/Prevention and consumer protection/financial integration?

To give a whole view of the process, the first chapter elucidates some basic aspects of money laundering and the stages involved in the process. Further on, the research takes place analyzing the global importance of money laundering prevention, along with the role of the FATF, and how all of that shaped up the current European framework in addressing the issue. On the second chapter, transaction monitoring was given a special emphasis because it constitutes itself as the first phase of money laundering prevention/control – genesis of automated alerts of unusual activities; it is also the technology current applied in financial institutions within the EU and because it illustrates the human-based decision-making throughout the whole process. Another key takeaway from the chapter was the need for transparency in given system. The third chapter elucidates the apparent conflict of two seemly public interest matters ML-FT/Prevention and consumer protection/financial integration. Some final notes are made on the conclusion.

1. BATTLE AGAINST MONEY LAUNDERING

In theory, money laundering is a straightforward concept. The person who has received ill-gotten earnings will want to ensure that they can spend these funds without others realizing that they are the product of improper conduct. To accomplish this, they will need to disguise the proceeds such that the original source of the proceeds is hidden, and the funds appear to be legal (Cox, 2014, p. 6).

Furthermore, money laundering can be concepted as the process of making a big sum of illegally obtained money appear to have come from a legitimate source. In that sense, criminals create the illusion that their ill-gotten funds are genuinely theirs to spend. It enables criminals to keep control of their unlawful gains and, eventually, to give a credible cover narrative for their source of income. Namely, it enables criminals to reap the benefits of their crimes. Money laundering often entails a series of transactions used as a smoke screen to conceal the true source of financial assets, allowing those financial advantages to be spent without exposing the culprits (Sullivan, 2015, p. 6).

When it comes to money laundering, however, there are normally two different connotations to consider. Money laundering refers to the employment of a business to assist the mixing of legal and criminal funds, as well as the more general process of concealing the original revenues of the funds, which is more commonly referred to as layering. By combining lawful and illicit funds, the full sum could potentially appear to be genuine and therefore laundered, meeting the money launderer's objectives. The funds will look to have originated from a legitimate business, but part of them will have come from criminal activities of some sort. Money laundering is critical in assisting the objectives of the drug dealers, terrorists, and organized crime, as well as many others who need to avoid the kind of attention from authorities that sudden wealth brings from illegal activity (Cox, 2014, p. 6).

1.1. CLASSIC TYPOLOGIES IN MONEY LAUNDERING

Money laundering is generally seen as a three-stage process, the notion is that the initial proceeds enter the financial system at a perceived point of vulnerability (the placement phase), and then the funds are shifted in such a way that the origin of the funds is concealed (the layering phase). The funds are finally reintegrated as clean funds into the mainstream banking system (the integration phase). Typically, money launderers concentrate on sections of the financial system with the least apparent oversight. Consequently, if the money launderer has specific knowledge that a person or business is in dire need of cash, this is likely to be an indication of an opportunity to be chosen for the initial placement of illicit funds. Due to the nature of the individual or organization's requirement, the level of due diligence may be decreased, allowing the money launderer to profit (Cox, 2014, p. 7).

The placement is the first step of the process. Also not being limited to the moving of funds into a bank account, despite this being the most commonly used process. The initial placement merely entails transferring the funds from their original cash source into another form, allowing the money launderer to perform additional layers and therefore conceal these amounts. Typically, money launderers concentrate on sections of the financial system with the least apparent oversight. Consequently, if the money launderer has specific knowledge that a person or business is in dire need of cash, this is likely to be an indication of an opportunity to be chosen for the initial placement of illicit funds. Due to the nature of the individual or organization's requirement, the level of due diligence may be diminished, allowing the money launderer to profit (Cox, 2014, p. 16).

After the initial placement of funds, the subsequent phase of the money-laundering procedure is the layering phase. As stated previously, the purpose of the layering phase is to obfuscate the proceeds of crime so that their origin and current location are unknown. Typically, this is accomplished by investing the illicit funds in something respectable, so that they now appear "clean." In other instances, a significantly more intricate set of transactions will be conducted. In more intricate schemes, the money launderer will shift the funds between several accounts in a number of different jurisdictions and through a series of corporations in order to obscure the trail as much as possible. This will jeopardize the audit trail and break the connection to the initial illegal proceeds. Prior to being deposited into the financial system, the cash can "spin" up to ten times in the most sophisticated instances of money laundering (Cox, 2014, p. 17).

Integration is the final step in the process of money laundering. It is the phase in which illicit proceeds are reintegrated into a legitimate financial system so that they can be amalgamated with other assets. This is where the criminally derived funds can be repatriated and used by the money launderer while appearing to be legitimate funds. Typically, money launderers will reintroduce "cleaned" funds into the system so that they look to have been acquired properly. The primary objective of the money launderer is to properly integrate funds so that it bec"mes dif"icult to discern between legitimate and illicit (criminal proceeds) funds, allowing them to be used for any purpose. There are numerous techniques to reintegrate money "hat has"been laundered into the legitimate economy. At this stage, the primary purpose of money laundering for the money launderer is to get his earnings without attracting attention or suspicion. The financial institution grows suspicious, and the culprit is subsequently identified when the money launderer abuses successful money-laundering tactics out of greed (Cox, 2014, p. 17).

Common methods of integration employed by money launderers include the following: One of the simplest means of integrating funds was to move money from a shell bank held by the money launderers to a legitimate bank. Shell banks, which conduct little genuine activity, are now routinely handled in jurisdictional rules, making this a more difficult sector to regulate. Money launderers are able to shift funds from one country to another by submitting inflated invoices for products and services. The invoices serve as proof of the origin of payments deposited with financial institutions. In nations where the right to privacy is guaranteed, money launderers can establish anonymous corporations. In the event of a future legal transaction, they are then allowed to award themselves loans using the money laundered. In addition, they will claim tax relief on the loan repayments and charge themselves interest on the loan, which may enhance their earnings (Cox, 2014, p. 19).

Another concerning method consists in the creation of anonymous corporations in countries where the right to privacy is protected. In the event of a future legal transaction, they are then allowed to award themselves loans using the money laundered. In addition, they will claim tax relief on the loan repayments and charge themselves interest on the loan, which may enhance their earnings. Another apparent example is the use of trading accounts at financial institutions. The money launderer deposits funds in an open brokerage account so that the financial institution can trade on their behalf. Later on, they remove the laundered funds from the account. After the premium has been paid, the money launderer may cancel an insurance coverage. The returned premium by the insurance firm is, of course, money laundering. The obtained assets may be sold on the open market or privately, with funds ideally deposited electronically into a valid bank account, which has been precisely launched, of course (Cox, 2014, p. 19).

These are only a few ways that the assets can be reintegrated into the normal economy. Typically, the goal of a money launderer is to get a cash payment from a genuine bank in order to deposit it into their account at another valid bank. Once this is accomplished, the laundering process is typically complete, and the criminal is free to utilize the funds for whatever purpose without fear of being caught (Cox, 2014, p. 19).

It is important to understand that there are two types of money laundering: professional and amateur. A professional money launderer will exploit any perceived hole in a financial institution's or regulatory structure's control measures. Amateur money laundering takes advantage of opportunities and does not disguise its tracks very well, leaving evident causes for concern that are easy to uncover either via employee diligence or through the use of modelling algorithms. Typically, law enforcement organizations discover the latter sort of money laundering, the professional, always more difficult and thus more expensive, to identify (Cox, 2014, p. 7).

Moreover, money launderers have not completely abandoned traditional typologies, classic and personal (Nunez Paz, 2011, p. 217). What seems to be the case is that these traditional typologies are now being combined with more sophisticated methods used to overcome the legal obstacles posed for the prevention of money laundering (Blanco Cordero, 2012; Souto, 2013).

In light of this, The Financial Action Task Force (FATF) is the primary group tasked by the world's seven major countries (G-7) with combating money laundering and terrorism financing around the world (Mekpor, 2018, p. 3).

1.2. THE FINANCIAL ACTION TASK FORCE

The UN's 1988 Convention against drugs and other similar substances, generally known as the Vienna Drug Convention, was the first worldwide reaction regarding the theme. The convention made offenders liable for prosecution if they were caught attempting to launder unlawful cash derived from the production and sale of narcotics. The Group of Seven (G7) established the Financial Action Task Force (FATF) in 1989 to confront the rising problem. The FATF broadened the definition of money laundering to include earnings from other unlawful activities such as illegal arms sales, insider trading, embezzlement, bribery, and fraud. Since then, in an effort to combat this expanding problem, the scope of money laundering regulation has been expanded on a regular basis, for example, to cover activities financing the act of terrorism (Tiwari *et al.*, 2020, p. 5).

The Financial Action Task Force (FATF) is an inter-governmental organization founded in 1989 by the Ministers of its member countries. The FATF's goals are to develop standards and support the effective implementation of legal, regulatory, and operational measures to combat money laundering, terrorist financing, and other risks to the integrity of the international financial system. As a result, the FATF is a "policy-making group" that strives to build the required political will to bring about national legislative and regulatory reforms in these areas. The FATF has created a set of recommendations that are widely accepted as the international standard for countering money laundering, terrorism financing, and the proliferation of weapons of mass destruction. They serve as the foundation for a coordinated response to these risks to the financial system's integrity and help to ensure a level playing field. The FATF Recommendations, first issued in 1990, have been amended in 1996, 2001, 2003, and most recently in 2012 to ensure that they stay current and relevant, and they are intended for universal applicability. The FATF evaluates its members' progress in adopting relevant measures, reviews money-laundering, terrorist-financing countermeasures, and also encourages the global adoption and implementation of appropriate measures. The FATF works with other international partners to identify national-level vulnerabilities in order to protect the international financial system from misuse (Cox, 2014, p. 29).

The FATF conducted a comprehensive assessment of its standards and published the revised FATF 40 Recommendations in February 2012. The purpose of this modification was to strengthen global safeguards and maintain the integrity of the financial system by equipping countries with more effective instruments to combat financial crime. Obviously, given the FATF has no legal authority in any country, this is an attempt to create a level playing field in financial crime and terrorist-financing prevention by establishing international best practice in the hope that this will put pressure on compliance. The proposals have been expanded to address perceived new dangers, such as the financing of the proliferation of weapons of mass destruction, as well as to be clearer on transparency and more stringent on corruption. The nine special suggestions on terrorist financing have been fully incorporated into the anti-money laundering mechanisms. This has resulted in a set of standards that are tougher and clearer, albeit mostly unaltered in many areas (Cox, 2014, p. 33).

In close collaboration with the FATF-Style Regional Bodies (FSRBs) and the observer organizations, including the International Monetary Fund, the World Bank, and the United Nations, the FATF has reviewed and updated the FATF Recommendations following the conclusion of the third round of mutual evaluations of its members. The amendments address new and emerging dangers, clarify and enhance a number of existing duties, and preserve the required stability and rigor of the Recommendations. In addition, the FATF Standards have been amended to increase the requirements for higher risk circumstances and to let nations adopt a more targeted approach in areas where high risks persist or where implementation may be improved. Initially, countries should identify, analyze, and comprehend the money laundering and terrorism financing dangers they face, and then they should take the necessary steps to reduce such risks. The risk-based approach enables governments, within the context of FATF regulations, to adopt a more flexible set of actions in order to target their resources more effectively and implement preventative measures according to the nature of risks in order to concentrate their efforts most efficiently (FATF, 2022, p. 8).

FATF is committed to maintaining a close and productive engagement with the private sector, civil society, and other interested parties as vital partners in protecting the integrity of the global financial system. The updating of the Recommendations has included considerable engagement and has benefitted from these stakeholders' views and ideas. In line with its mission, the FATF will continue to review, as necessary, modifications to the standards in light of new information regarding emerging risks and vulnerabilities to the global financial system. FATF urges all nations to adopt effective steps to bring their national systems for fighting money laundering, terrorism funding, and proliferation finance into conformity with the amended FATF Recommendations (FATF, 2022, p. 9).

It has now become a classic statement that the methods and techniques used for money laundering “are in constant evolution” (FATF, 2011a). There were also arguments in favor of the "balloon effect," a phrase developed to explain how criminals adapt when police impede some money-laundering processes by employing alternative methods. Thus, as national and international prevention and prosecution mechanisms choke off specific money laundering techniques, the "scope" shrinks in that areas but expands in other parts (Zagaris, 2010). No doubt, “ease of adaptation to new situations and speed the development of new methods” (Blanco Cordero, 2012) is a fundamental characteristic of money laundering (Souto, 2013).

FATF has given particular attention to trust and corporate service providers in recent years (FATF, 2010a). Their crucial function as intermediaries between financial institutions and their consumers has repeatedly been used for illicit money laundering purposes. As also stated by letter e of the 22nd amended FATF proposal (2012), trust and business service providers can play a significant role in discovering, deterring, and punishing all people and organizations engaged in the establishment, administration, and management of funds (FATF, 2012). The creation of the trust has made it possible for money launderers to hide their identity by setting up a fund, so that it is shown that the trust company is seemingly the one performing the operations (Collado Medina, 2010). Money launders can also utilize an NGO, association, foundation or non-profit organization to channel criminal assets by leveraging its tax-exempt, non-profit (Chinchilla, 2011), donations anonymity and greater laxity in controls due to charitable reasons (Collado Medina, 2010; Souto, 2013).

FATF was also concerned about the financial flows associated with organized maritime piracy and abduction for ransom (FATF, 2011d), both of which have increased dramatically in recent years, particularly off the coast of Somalia (FATF, 2011a). FATF has researched the connections between corruption and money laundering (FATF, 2011b, 2012b), based on actual incidents in which corrupt officials transferred money in secret, as well as the difficulties in collecting the proceeds of corruption after they have been identified (FATF, 2011a). FATF has also focused on inhuman trafficking and illegal immigration (FATF, 2011a), one of the most lucrative criminal phenomena (FATF, 2011a) obviously linked to money laundering, and has even shown interest in football, where economic growth has become exponential, making it an attractive sector for money launderers (FATF, 2009a). The FATF also examined the 3,000 free trade zones that have been established in 135 countries. Money launderers can take advantage of the same attributes that make these places desirable free trade zones for legitimate enterprises by easing trade and financial constraints (FATF, 2009a; Souto, 2013).

Furthermore, the FATF has always been concerned about its recommendations being applied "not only to banks but also to non-bank financial entities" (FATF, 1990) such as exchange offices and insurance companies, and this worry has not faded over time. Specifically, the sector of foreign exchange and money remittance devoted a special report in 2010 that demonstrated with the use of various examples, voluntary or unconscious, laundering activities and warned the detection at low compared to the volume of suppliers (FATF, 2010b). Among these alternative delivery systems are hawala and hundi, informal funds transfer without moving based on a trust relationship, and voucher systems in China and East Asia (Collado Medina, 2010). FATF also hosted the insurance industry in 2009 with the intention of fostering dialogue between authorities, insurers, and intermediaries for the prevention of money laundering Spanish criminal reform 269 via an effective system based on the identification of risks and difficulties (FATF, 2009b; Souto, 2013).

Similarly, the FATF expanded, in its 2012 recommendation number 22, the requirements of due diligence on customers and information record of the 10th, 11th, 12th, 15th, and 17th recommendations to the following professions and no financial businesses: casinos, real estate, dealers of precious metals and stones, attorneys, notaries, other independent legal professionals, accountants, and trustees (Souto, 2013).

Regarding casinos, they are necessary only when consumers conduct transactions worth at least 3,000 euros or dollars, but identification at the casino's door may not enough for a number of other transactions (FATF, 2012). In 2008, the FATF issued recommendations on casino-related threats (FATF, 2008a), and in 2009, it issued a comprehensive study on gaming sector and casino vulnerabilities. In this research, the FATF highlighted currency exchange and structuring operations, the complicity of staff, chips, checks, and casino accounts, and presented indications that might aid in identifying and preventing money laundering (FATF, 2009c). These guidelines are intended to combat casino-related instances of money laundering dating back to the 1920s. Notably, Al Capone worked between American and Cuban casinos in the 1920s. Money laundering can be accomplished by acquiring chips that are not utilized in the game (Chinchilla, 2011) and then exchanging them for legal-appearing cash or checks (Souza, 2012). The technique is one of the "most common mechanisms" (Jurado and Garca, 2011) for money laundering and exploits the absence of control in casinos over the chips that are purchased and played (Ferro Veiga, 2011). According to the 2009 FATF Report, millions of pounds were laundered between the United Kingdom and Dubai via a casino (FATF, 2009c; Souto, 2013).

The 2009 report does not address illegal gambling (Shehu, 2004) or online gambling (Hugel and Kelly, 2002, comparing the US and UK governmental policies on internet gambling), but in the future, due to the relationship between money laundering and regulated online gambling, more attention should be paid to their development (Brooks, 2012). Ways to strike a compromise between individual privacy and the interests of law enforcement should also be considered (Mills, 2001). Insofar as real estate agents pose a risk of money laundering (FATF, 2008b), they are subject to the recordkeeping requirements and diligence when participating in the sale of properties to their clients and must comply with the tenth recommendation's requirements for both buyers and sellers of goods (FATF, 2012, recommendation 22nd; Souto, 2013).

As for traders in precious stones and metals, they are required to do client due diligence and record cash transactions over 15,000 euros or dollars in one or more connected transactions (FATF, 2012). They are also expected to report suspicious cash transactions equal to or exceeding this threshold, under recommendations 18 through 21. (recommendation 23rd). Gold, precious stones, and metals are not included in the 32nd recommendation on cash couriers, despite their high liquidity and use in certain situations as a medium of exchange or transfer value, and despite the fact that states, prior to the discovery of unusual movements of these goods, should notify the authorities of the origin and destination of the shipment and cooperate in stating the purpose of the movement and in the adoption of measures (FATF, 2012). Concern about this sector is more than warranted (FATF, 2008b), as the use of precious stones and metals by traders is one of the most common mechanisms of money laundering (Jurado and Garcia, 2011), as evidenced by the discovery of gold in investigations of money laundering involving the Russian mafia in Italy (Varese, 2012; Souto, 2013).

Regarding the beneficiaries of accounts or transactions, the FATF initially encouraged financial institutions to take reasonable measures to investigate the true identity, a requirement from February 2012 stated in recommendation 10th, as money launderers typically use banks for deposits and subsequent transfers (Chinchilla, 2011; Jurado and Garca). There is evidence that even a robust identity and verification system may be circumvented by utilizing third parties, such as straw men (FATF, 2010b). As for the identification and monitoring of transboundary financial flows, while being one of the oldest methods of money laundering, their volume continues to drastically expand (FATF, 2010b). Thus, according to a newly released assessment of the structure of the Mafia by VARESE, illegal products entered Italy via a vast network of persons who traveled from Russia with cash (Varese, 2012). There are also new "money mules" recruited by email under the guise of having internet-based chances to work from home; the only recompense they sometimes receive is criminal prosecution for money laundering (Clough, 2010; Souto, 2013).

Lastly, the 32nd suggestion advises countries to guarantee that their authorities obstruct or prohibit the transfer of suspected money laundering-related funds (FATF, 2012a). According to Jurado and Garca (2011), cash is the most prevalent means of exchange in illegal activities. In a similar vein, the Spanish government, mindful of its tax collection objectives, approved in the council of ministers on 22 June 2012 a bill to combat tax fraud, based on the legislative experience of other EU countries such as France and Italy, limiting cash transactions involving businessmen or professionals to 2,500 euros (Ley 7/2012, 2012, article 7). To escape the Charybdis of paper currency, however, we shall encounter the Scylla of "electronic money," since modern payment technologies, as seen in the preceding section, are not without problems that may obstruct money laundering detection and suppression. Moreover, the seeming doctrine of the "criminogenic nature of cash" conceals an agenda that goes beyond the battle against crime, further marginalizes individuals with lower incomes, and permits control of the private sector (Pieth, 1992; Souto, 2013).

Furthermore, the Basel Committee on Banking Supervision, sitting within the Bank for International Settlements, is the leading global standard-setter for worldwide banking regulation and supervision. Its mandate is to strengthen the regulation, supervision and practices of banks worldwide, with the purpose of enhancing financial stability. In full support of the Financial Action Task Force Recommendations, the Committee issued a paper enti- tled *Sound management of risks related to money laundering and financing of terrorism* in January 2014, which provides a framework of regulatory best practice broadly based on the FATF Recommendations. The paper enunciates the three lines of defense against money laundering (Cox, 2014, p. 55).

The paper asserts that client-facing front-office personnel should be considered the first line of defense against financial crime. They are responsible for detecting, analyzing, and controlling the risks of their business and should be provided with adequate resources and knowledge of the relevant policies and procedures. The responsibilities are shared by both the staff, who must remain vigilant at all times to apply the principles without alerting the clients, and the senior management, which must select the appropriate staff and ensure that they have adequate guidance and training to carry out their assigned roles (Cox, 2014, p. 55).

The second line of defense against money laundering consists of the senior management and compliance staff. The chief officer in charge of AML/CFT should be responsible for overseeing the bank's continuing compliance with all AML/CFT obligations. This requires sample testing of compliance and evaluation of exception reports in order to warn senior management or the board of directors if it is thought that management is not addressing AML/CFT processes responsibly. The chief AML/CFT officer should be the point of contact for internal and external authorities, including supervisory agencies and FIUs, on any AML/CFT-related matters (Cox, 2014, p. 55).

This may be a nice concept in theory, but its implementation will differ depending on the size of the organization. The chief AML officer of a large organization will find it particularly challenging to monitor all AML duties; hence, this responsibility is typically transferred to front-office employees (Cox, 2014, p. 55).

The internal audit function offers the third line of defense and plays a crucial role in reviewing risk management and controls independently. It discharges their duty to the audit committee of the board of directors or a comparable oversight body by conducting periodic assessments of the efficacy of compliance with AML/CFT policies and procedures. A bank must establish policies for conducting audits of (a) the adequacy of the bank's AML/CFT policies and procedures in addressing identified risks; (b) the effectiveness of bank staff in implementing the bank's policies and procedures; (c) the effectiveness of compliance oversight and quality control, including parameters for automatic alerts; and (d) the effectiveness of the bank's training of relevant personnel. Senior management should guarantee that audit functions are assigned personnel with the necessary expertise and experience to undertake such audits. Additionally, management should verify that the audit scope and methods are adequate for the bank's risk profile and that the audit frequency is likewise risk-based. Periodically, internal auditors should undertake bank-wide AML/CFT audits. Moreover, internal auditors must be proactive in implementing their findings and suggestions. In general, auditing processes should adhere to the internal audit's broader audit mandate, subject to any auditing standards applicable to AML/CFT measures (Cox, 2014, p. 55).

In conclusion, while this is an essential component of the AML deterrent regime, the hands-off, reactive, and sporadic character of internal audit means it may be too late by the time any suspicious behavior is discovered. This layer of defense instead seeks to fill any holes in the first and second lines of defense (Cox, 2014, p. 55).

1.3. THE RATIONALE OF MONEY LAUDERING CONTROLS

Given the continual increase in the scale of Money Laundering, compliance costs have increased by a rate of 53% globally for just banking institutions and show no indications of slowing down (PricewaterhouseCoopers, 2014). Furthermore, the United Nations Office on Drugs and Crime's biennial budgetary allocation for AML activities in 2014-2015 was $760.1 million, which included approximately $88.9 million (11.7 percent) from the UN's regular budget (Mekpor, 2018, p. 3).

The latest data breaches, such as the Paradise Papers, Panama Papers, and Offshore leaks, have focused attention on the scope and impact of money laundering activities on a global scale. As a result, understanding the work done around issues on a worldwide scale becomes critical (Tiwari *et al.*, 2020, p. 5).

In light of this, a new era of globalization has begun, which is uniting continents and reshaping local politics and international relations. Globalization necessitates an international convergence of knowledge, capital, and technology, resulting in a single global market and, to a considerable extent, a global village. Despite the various benefits of globalization, the same characteristics of globalization that have extended chances for free-market capitalism over the world have also resulted in new threats. Among these dangers is an increase in the prevalence of money laundering and terrorist financing (Mekpor, 2018, p. 1).

According to the estimates of the United Nations, illegal cash flows were around $2,100,000,000,000,000 in 2009 or nearly 4% of world GDP. The profits of crime are initially concealed and subsequently reinvested in Member States that are unrelated to the location where the crimes were committed. In fact, this is how transnational organized crime distorts competition, destroys faith in the financial system, and depletes the Member States' and Union's budget of tax revenues. The more our systems of seizure and confiscation of criminal assets and Asset Recovery Agencies remain underdeveloped, the more illicit firms will be able to create unlawful gains and severely impact the Internal Market (Ioannides, 2014, p. 27).

According to Europol, money laundering is the culmination of all sorts of organized criminal activity, it is essential in assisting the objectives of the drug dealers, human traffickers, terrorists, and tax evaders (EUROPOL, 2006).

All the more reason for anti-money laundering policymakers in the European Union to preserve the Union's linked financial markets by prosecuting all activities that generate illegal wealth. The current trend is to investigate, prosecute, and punish all forms of illicit enrichment (corruption, tax evasion, private corruption, insider trading, misuse of money, market abuse, counterfeiting, and piracy), including criminal infiltration of financial institutions and businesses (Ioannides, 2014, p. 19). Money laundering, in addition to the major dangers stated above, weakens the integrity of the private sector (Unger *et al.*, 2012), undermines democracy and the rule of law (Diamond, 2016), and causes reputational damage (Unger, 2014). Anti-money laundering (AML) policy extends back to the 1980s, when governments and corporate players recognized the need to confront money laundering's disease (Mekpor, 2018, p. 3; Verhage, 2009).

Furthermore, numerous individuals and businesses believe that Anti-money Laundering and Combating the Financing of Terrorism are overestimated. According to Savona (2005), "the economic cost of controls based on obligations and prohibitions is often underestimated, while the benefits they produce are frequently exaggerated." Geiger and Wuensch (2007) also stated that AML legislation might lead to a distortion of competition between businesses, which poses a threat to enterprises globally since it could slow the development of society toward wealth creation and reduce the yearly productivity of firms. They said that AML fees are superfluous transaction costs that hit the majority of banks, with smaller banks bearing the burden twice as much as larger institutions. Others argue that it is not AML in its generic meaning that is superfluous, but rather the existing techniques employed in AML programs (Beekarry, 2011; Mekpor, 2018, p. 7; Turner, 2004).

The most significant benefit of AML Compliance is that it protects the global financial system's integrity. Compliance is described by Young (1979) as "the actual behavior of a given subject conforming to prescribed behavior." Young (1979) claimed that noncompliance arises when real conduct considerably deviates from prescribed behavior. Consequently, AML Compliance may be described as any measures taken by reporting institutions that adhere to the standards, rules, objectives, laws, and regulations established by authorities to combat money laundering (Choo *et al.*, 2014). As the strategies employed by money launderers evolve, so do the FATF Recommendations in order to handle contemporary trends. According to Putnam (1988), the effectiveness of a worldwide AML/CFT framework is largely dependent on the effectiveness of its components, and vice versa. Putnam (1988) argues further that global collaboration should be viewed as a "two-level game" in which the compliance of local governments with AML Policy is viewed as the first step toward a successful global AML Policy (Mekpor, 2018, p. 8).

Yepes (2011) states that while progress has been made across the major areas of the 40+9 FATF Recommendations, compliance with the AML/CFT Standards is typically poor across the globe. This finding was obtained in a research that analyzed nations compliance with FATF recommendations across borders. Yepes (2011) discovered in his analysis of 87 countries that institutional characteristics have a significant impact on AML compliance. Institutional variables have a crucial role in AML compliance, according to Yepes (2011), since they create the conditions under which policy reforms or amendments are established and thus accommodate, constrain, or diverge their implementation. Existing research identifies significant characteristics that either facilitate or impede AML Compliance (Mekpor, 2018, p. 8).

1.4. EU AML/CTF FRAMEWORK

The transfer of clean money is not unlawful nor prosecutable. There is no place for anonymity in financial transactions involving property in a fungible form derived from legal sources. Nonetheless, the genuine need to protect national security, public safety, financial integrity and stability, and overall economic well-being has become so compelling that today's financial regulators can only fulfill their enforcement responsibilities by implementing anti-money laundering controls on the blueprints of financial activities conducted via financial intermediaries at the national and cross-border levels. The mandatory rules of financial regulation are highly peculiar, if not socially objectionable, as they stipulate that suspicion can be eliminated only if two specific criteria are met: documentary evidence of the legal sources of the funds involved and the establishment of innocent financial and commercial motives on the part of the parties to the transaction. In summary, when suspects fail to publicly, rationally, and truthfully explain the legal sources of the property they manage, hold, and control, the suspicion of criminal culpability cannot be erased and will thus become the subject of legal proceedings (Ioannides, 2014, p. 3).

The imposition of the aforementioned two obligations on natural and legal persons, as any jurist would confirm, not only reveals the confidentiality of financial and commercial transactions, but also consolidates the legal extroversion of two diametrically opposed forces that establish innocence or guilt in the context of anti-money laundering law: the statutorily guaranteed confidential submission of self-induced suspicion by reporters and the publicly offered reasonable and truthful explanations on the part of those who have been reported for alleged wrongdoing. In light of this, it is essential to recognize that these two opposing forces will vividly depict the suspect's or even the accused's picture of innocence or guilt in the following five phases of money laundering prevention and control: genesis of automated alerts of unusual financial activities; internal processing of the findings of suspicion by financial institutions; submission of Suspicious Activity Reports as disclosures of alleged offences to financial intelligence units (triggering the investigation of the financial affairs of suspects); confidential and compatible with the ECHR financial investigations of suspects; and prosecution of suspects for money laundering, the bringing of the indictment for the offences, and trial (Ioannides, 2014, p. 3).

In light of the aforementioned arguments, it is helpful to realize that anti-money laundering legislation are 30 years old. Systematic legal study over the past three decades has conclusively proved that money laundering constitutes illegal financing. The criminal culpability of those who conspire to launder money is very stringent. Despite the fact that modern financial regulation enables us to keep an eye on evolving transparency laws, it does not always make sense to the untrained eye that the prevention and control of economically motivated serious crime is solely concerned with human greed, self-interest, and what theologians might refer to as the propensity of the morally weak to be seduced by Mammon (Ioannides, 2014, p. 3).

Paradoxically, the heterogeneous criminal, civil, and tax laws of European Union Member States are constantly being strengthened to combat all forms of illicit enrichment, while wrongdoers, organized criminals, and those involved in terrorist financing schemes are constantly preoccupied with discovering systemic weaknesses or inventing new techniques to circumvent the controls of anti-money laundering legislation and to corrupt those in positions of authority (Ioannides, 2014, p. 3).

Also, there is a compelling public interest in ensuring that credit and financial institutions, businesses, and certain professions vulnerable to the corruptive forces of organized crime and money laundering not only report suspicious activities, but also serve as the watchful eyes of investigative and judicial authorities. On the other hand, it should be noted that this third expansion of the global anti-money laundering regime to combat and punish terrorism funding has generated major issues about the need to increase the transparency of the anti-money laundering and counter-terrorism financing system (Ioannides, 2014, p. 19).

Moving on, Emmanuel Loannides enunciates 12 conceptual objectives regarding money laundering countermeasures, especially aiming to:

i. Protect and promote the stability, integrity and reputation of the financial system[2] and, at the same time, protect citizens against crime and terror.[3]

ii. Provide a disincentive to economically motivated serious crime through the

iii. reduction of profit (Hinterseer, 2002) and the drastic decrease of the inflow of dirty money that can finance further crime and terror (Rider, 1996a, 1996b, 1996c).

[2] Council Directive 91/308/EC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering [1991] OJ L166/77, articles 3–4; Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering – Commission Declaration [2001] OJ L344/76.

[3] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist activity [2005] OJ L309/15, preamble and articles 1–13; Naylor (1987, p. 367).

iv. Provide effective tools for the conviction of money laundering offenders

v. and the prosecution of predicate offences through the international network of Financial Intelligence Units assembled by the Egmont Group; and the engagement of financial institutions in the fight against money laundering (Her Majesty's Treasury, 2007).

vi. Make criminal wealth vulnerable upon it entering the formal economy (European Union, 2008a), assist in the rapid tracing of criminal assets, and promote civil recovery action domestically and abroad.

vii. Eradicate to the maximum possible degree unfair competition (European Union, 2008b), corporate and financial malpractice (European Union, 2006), market abuse and insider dealing (European Union, 2009), fraud (European Union, 2007) and tax evasion (European Union, 2008c).

viii. Provide a new generation of more intelligent and cost-effective tracing technologies for illegal proceeds. Member States are expected to use these instruments within the context of a plan based on the principles of effectiveness, proportionality, and participation of public and private sector partners (Ioannides, 2014, p. 8).

ix. Facilitate the extraction of information from private sector stakeholders concerning the identity of those persons engaged in apparently suspicious transactions and, at the same time, provide for a system of multiple checks of commercial, financial and personal data by law enforcement and intelligence agencies at the national, regional and international levels (Ioannides, 2014, p. 8).

x. Provide a mechanism for the continuous revision and clarification of universally adopted proactive and reactive tools against the laundering of criminal proceeds; increase the level of accountability and private sector engagement; and promote the sharing of knowledge and understanding of newly emerging typologies of money laundering and terrorism financing activity (Ioannides, 2014, p. 9).

xi. Tighten controls on persons holding positions of trust in the public and private sectors and, more specifically, prevent corrupted political leaders from siphoning off taxpayers' money. The deeper notion of this objective has to do with the prevention and control of the accumulation of unaccountable wealth in the wrong hands and the prevention and control of illicit enrichment as a whole (Ioannides, 2014, p. 9).

xii. Promote and enhance good governance, best practices, transparency and corporate social responsibility.

xiii. Increase financial regulatory and law enforcement activity in regard to capital flight from *hot* areas through the informal value transfer system,[4] and assist in resolving the problem of how funds are actually transferred from the European Union to destinations such as North Africa without traceable money transfer orders.[5]

xiv. Enhance the international initiatives to improve poor governance[6] and combat systemic corruption (European Commission, 2012) in non-cooperative countries and territories.[7]

The growth of money laundering and terrorist funding, coupled with tax evasion and state austerity programmes, has pushed the fight against money laundering and financial crime onto the political agenda of the European Union (EU). This has caused the European Commission to issue a slew of guidelines. The overarching goal of all of these instructions was to prevent unlawful use of the global financial system. The many EU anti-money-laundering directives are the means by which the EU combines the FATF's international standards in order to create cohesive anti-money-laundering legislation, while underlining unique extra problems of importance to EU

[4] Text to n 8 Question 255 of Lord Jopling addressed to witness Professor Gilles de Kerchove, European Union Counter-Terrorism Coordinator, on the Hawala system of informal remittances.

[5] Text to n 8 Question 257 of Lord Jopling to which Professor de Kerchove responded by making reference to the North African communities in Europe transmitting money to North Africa without traces.

[6] Text to n 8 Question 391 of Lord Richard to which Sir James Sassoon stressed that the involvement of the International Monetary Fund and the World Bank in ensuring implementation of the Financial Action Task Force global standards would actually put pressure on countries whose financial governance is poor to put their houses in order.

[7] Text to n 8 Question 417 of Lord Hannay of Chiswick on the role of Non-cooperative countries and territories to which Sir James Sassoon responded by referring to the northern part of Cyprus, Uzbekistan and Iran.

legislators. As with all EU directives, national governments are required to translate these criteria into local legislation (Cox, 2014, p. 61).

The purpose of the First EU Money Laundering Directive (1991) was to prevent the laundering of narcotics profits through the banking sector. The Directive stipulated that enterprises in the financial sector must maintain systems for client identification, employee training, recordkeeping, and the reporting of suspicious transactions. The Second Money Laundering Directive (2001) revised the First Money Laundering Directive by providing modifications in two major areas. First, it broadened the area of predicate offenses for which mandatory suspicious transaction reporting was required from drug trafficking (the First Directive) to all serious offenses. Second, it broadened the scope of the Directive to cover non-financial businesses and professions, such as attorneys, notaries, accountants, real estate brokers, art dealers, jewelers, auctioneers, and casinos (Cox, 2014, p. 61).

The Third Directive recognizes that, by Its very nature, money laundering is an international issue that must be tackled at the international level. It recognizes that national anti-money-laundering efforts can never be completely effective. Therefore, international coordination and collaboration are required for consistent international action to address money laundering and terrorist financing successfully (Cox, 2014, p. 61).

The European Community has given special consideration to the FATF Recommendations as a foundation for achieving its goals. The Third Directive offered a uniform basis for executing the 2003 FATF Recommendations, which were amended in 2012. The 2003 guidelines considered the new risks and practices that had emerged since the last Directive (the Second Directive). In addition, the Financial Services Authority, the UK's regulatory authority at the time, and other international regulatory bodies intended to use a risk-based strategy to counter money laundering. Through cost–benefit analysis, the Third Directive also sought to verify that these additional requirements were realistic, reasonable, and justifiable (Cox, 2014, p. 61).

The third Directive is focussed on streamlining, clarifying and harmonising the second Directive, such as expanding the scope of the risk-based approach, and harmonising the criminalisation of the money-laundering and terrorist-financing offences, by providing a transparent method for identifying beneficial owners. In addition, firms will be compelled to keep records of the identities of individuals who are actually behind the business. Also by enhancing the clarity and transparency of the rules on customer due diligence in order to implement suitable controls and procedures that ensure a better understanding of clients and their business nature. Particularly, it is essential to ensure that streamlined procedures are not mistakenly interpreted as complete exemptions from client due diligence. In addition to "foreign" and "international" politically exposed persons and those in international organizations, "domestic" politically exposed persons (those resident in EU Member States) are now included in the regulations pertaining to "politically exposed persons." This comprises, among others, heads of state, government officials, legislators, and supreme court justices (Cox, 2014, p. 61).

The Third Directive provides Member States with the regulatory framework they need to address the prevention of money laundering and funding of terrorism. Each Member State must thereafter develop regionally applicable measures to execute these criteria. As a result, any foreign authority might utilize the Directive as a template for developing its own laws and regulations. You may thus regard the Directive to be worldwide best practice even if you are not located in a Member State. It is crucial for every jurisdiction to recognize that the Directive gives only general information and must always be reinforced by appropriate local guidance and incorporated into local legislation. As a result, while it offers the framework, it is unable to provide specifics owing to changes in local rules, regulations, and institutions (Cox, 2014, p. 61).

Significant modifications were made with the fourth Anti-Money Laundering Directive, including that transactions in excess of EUR 7,500: The threshold for merchants of high-value items receiving cash payments and traders conducting occasional transactions to conduct due diligence will be lowered from EUR 15,000 to EUR 7,500. This is in response to allegations from Member States that the EUR 15,000 threshold was being abused by criminals, and it is hoped that by halving it, criminals will have fewer opportunities. Details pertaining to the beneficial owner: The amended Directive proposes new measures to increase the transparency and accessibility of beneficial ownership information. It requires legal entities to keep track of their beneficial ownership information. This information must be made accessible to both competent authorities and required entities. For legal arrangements, trustees are required to declare their position when becoming a customer, and beneficial ownership information must also be disclosed to competent authorities and obliged entities. This provision signals a crackdown on the use of corporate structures to conceal financial crime and is introduced at a time when courts routinely question the viability of penetrating the corporate veil (Cox, 2014, p. 61).

Risk-based approach: The Fourth Money Laundering Directive introduces the risk-based approach as a balance between financial crime deterrence and economic stability. While this has been the position of the United Kingdom since the Money Laundering Regulations were introduced in 2007, adopting a risk-based approach aligns the Directive with the FATF Recommendations.

Streamlined and improved due diligence: In accordance with the plan, obligated entities would be required to take more stringent precautions when the risks are higher, and they may be entitled to take less stringent precautions when the risks are proved to be lower. Politically exposed persons: The definition of PEPs will be enlarged to include domestic PEPs in recognition of the inherent danger associated with dealing with PEPs. The gambling industry: The standards for consumer due diligence are expanded beyond casinos to the broader gambling industry. This is hardly surprising given the tremendous expansion of the mobile/in-play gambling business (Cox, 2014, p. 61).

Frequently, cryptocurrencies are used for money laundering and financing terrorism.[8] Their decentralized and pseudonymous structure makes them ideally suited for such illegal activity. Thus, cryptocurrencies and their related services must be controlled within the existing anti-money laundering and counter-terrorism funding framework (AML) (Haffke *et al.*, 2020).

European politicians addressed this issue. Directive (EU) 2018/843, sometimes known as the Fifth Anti-Money Laundering Directive (AMLD5), modifies

[8] For example, see Financial Action Task Force (FATF, 2018, p. 2); HM Treasury and Home Office (2017, p. 40), stating that the risk for money laundering is growing; Haffke *et al.* (2020); Teichmann (2018).

the existing legal framework to particularly address the AML concerns posed by cryptocurrencies (Haffke *et al.*, 2020). By January 2020, Member States must incorporate relevant provisions into national legislation. Currently, national consultations on the Directive's implementations are scheduled or underway. The Financial Conduct Authority (FCA) of the United Kingdom has indicated that it is likely to exceed the scope of the Directive (Haffke *et al.*, 2020).

The fourth money laundering Directive (EU) 2015/849 does not require cryptocurrency exchanges, crypto marketplaces, wallet-providers, or tumbler services to register. [9] If their operations do not come under the scope of any other obligated body, they are exempt from AML responsibilities under existing European Union legislation. For instance, they are not required to identify their consumers via KYC (Know-Your-Customer) procedures. In addition, they are not required to disclose any questionable transactions (Haffke *et al.*, 2020).

Due to the fact that cryptocurrency transactions are conducted using pseudonyms, this circumstance should be significantly changed. By enacting AMLD5, European Union lawmakers sought to ensure that competent authorities of Member States "are able to monitor the usage of virtual currency through obliged entities."[10] Recognizing that (quasi-)anonymous transactions are feasible outside the aforementioned services through private transactions, the strategy is to collect as much information as possible for national authorities (Haffke *et al.*, 2020).

Consequently, two new obligated entities are introduced: "Providers engaged in exchange services between virtual currencies and fiat currencies" [11] and "providers of custodial wallets.[12] The latter are defined as "an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies"[13] Both entities are denoted by the phrase "virtual currencies," which is specified by Article (1) (2) (d) of AMLD5 (Haffke *et al.*, 2020).

[9] See AMLD5 Rec. 8; Houben *et al.* (2018, p. 62); Vandezande (2018, pp. 286, 298-303, 309-310), also citing the view of the European Commission.

[10] AMLD5 Rec. 8.

[11] AMLD5 Art. 1(1)(c); AMLD4 Art. 2(1)(3)(g) in its amended version.

[12] AMLD5 Art. 1(1)(c); AMLD4 Art. 2(1)(3)(g) in its amended version.

[13] AMLD5 Art. 1(2)(d); AMLD4 Art. 3(18) in its amended version.

AMLD5 aims to enable Financial Intelligence Units (FIUs) to "to obtain information allowing them to associate virtual currency addresses to the identity of the owner of virtual currency.” [14] The identities of currencies and their virtual currency wallets will not be registered or made public. Rather, it is the responsibility of the European Commission to evaluate the need for such a registry by January 2022.[15] AMLD5 intends to enable FIUs to collect the required information to address money laundering threats associated with virtual currencies (Haffke *et al.*, 2020).

Without the systematic extraction of financial intelligence data from private sector players, neither the reporting system nor the interchange of information can function. This richness of information is not only the foundation for financial intelligence, but also the foundation for law enforcement and judicial agencies to successfully battle money laundering, the financing of terrorism, and corruption The (The Egmont Group, 2009).

Therefore, we must always keep in mind the following three fundamental concepts that the reporting system entails Ioannides (2014, p. 24). Turning private sector stakeholders into secret reporters; transforming financial institutions and enterprises into the eyes of law enforcement and prosecutorial authorities; and transplanting to reporters a sophisticated, qualitative and systemic undercover reporting culture.

Nonetheless, it is of equal importance to emphasize that the factual evidence of successful reporting (Suspicious Activity Reports – Tactical and Strategic Analysis – Exchange of Information) facilitates the application of multiple controls by law enforcement authorities, for the prosecution and sanction of various crimes, and at all levels of cooperation (national, regional, and international) to combat money laundering and the financing of terrorism. Nevertheless, the transmission of information through the secure channels of Financial Intelligence Units, which is the intelligent byproduct of intelligence collecting that is first prompted by automated or self-induced suspicion, intends to promote effective assistance in transnational criminal investigations (Ioannides, 2014, p. 24). On the other hand, the security of sensitive commercial,

[14] AMLD5 Rec. 9.

[15] AMLD5 Art. 1(41); AMLD4 Art. 65(1) third sentence in its amended version.

financial and personal data processed by Financial Intelligence Units, cannot be used as acceptable evidence in court proceedings owing to its highly confidential nature.

2. TRANSACTION MONITORING

In order to avoid fines, financial institutions today place a significant emphasis on getting their house in order and establishing a Compliance program that satisfies the regulator. Nonetheless, and somewhat ironically, the more the examination of transactions, the greater the operational expenses, especially when effective monitoring and avoiding the unnecessary reporting of genuine customers requires human intervention at some stage in the process. AML activities are expensive from both a human resource and an IT standpoint. All of these factors are eating away at the bottom line and may have an impact on both profitability and shareholder value. From the standpoint of a publicly registered, profit-driven financial institution, the fundamental objectives of AML operations boil down to achieving the optimal balance between overreporting and underreporting in the most cost-effective manner. This is the primary goal of any AML automation (Chau *et al.*, 2020).

The automated monitoring of AML transactions is a sort of predictive analysis. Based on a restricted collection of facts that, in and of itself, will never be conclusive as to whether or not a transaction constitutes money laundering or is part of it, the system attempts to filter circumstances to guide the analyst in the appropriate path. A human analyst will ultimately examine the generated warnings to evaluate whether the technology appropriately identified the condition. This might be the compliance analyst of the financial institution, his or her colleague or boss, an internal audit team, a regulatory watchdog audit team, or the FIU analysts to whom really suspicious incidents are reported (Chau *et al.*, 2020, p. 29).

If an alert is deemed irrelevant or insufficiently suggestive of money laundering, this is referred to as a false positive. Depending on the stage of the procedure, a false-positive result might have numerous meanings. Let's go over the most typical procedure to determine what counts as a false positive at each stage. After alert generation, the majority of financial institutions begin the process with an AML analyst performing initial triaging. Many Compliance departments (and the same is true for fraud investigation) differentiate between an alert and a case, with the latter meaning that one or more alerts are singled out for additional scrutiny and more time and effort is spent determining whether or not these alerts should be reported to the FIU. When an analyst disregards the signal, this will be a false positive, or false alarm, from his or her perspective (Chau *et al.*, 2020, p. 29).

It is commonly known in both AML and fraud that nine out of ten alerts are false positives. At this level, a true positive indicates that the alert may be possibly reportable; hence, either reporting will be determined or, as is typical, a case will be launched to further investigate. The case investigation can be conducted by the same analyst who has decided to commit more time to it, but many financial institutions have formed a distinct investigator or senior analyst position for that purpose. At this point, the same question is asked again: Are the alerts under examination sufficiently inconsistent with what would be expected under the same circumstances to justify informing the authorities? Here, a true positive indicates that the FIU must be provided with information about the account's transactions and account holders. Positive alert here equals regulatory report (Chau *et al.*, 2020, p. 28).

From one perspective, the ratio of cases produced to reports filed increases as the analyst's performance improves. This procedure will be repeated at the level of the Financial Intelligence Unit (FIU), which will investigate the incoming reports, connect them where applicable, and send them over to law enforcement, which in many nations consists of specialized financial investigative units. True positive here refers to a report worthy of additional examination by the FIU, which will ultimately result in a prosecution-worthy case. A real positive alert signifies that the final money launderers and those who benefit from the money laundering operation are convicted in court and the verdict is sustained in appeal (Chau *et al.*, 2020, p. 28).

Clearly, financial organizations often do not care about this legal follow-up. At most, the prosecution requests documents as evidence in their case, the financial crimes unit collaborates with the bank's fraud prevention department in investigations, and/or bank personnel are called to court to testify. In the early phases of triage, case investigation, and report submission for financial institutions, it is assessed if an alert is genuine or fraudulent. Nonetheless, it is essential to recognize that the concept of a false positive and the false positive rate, as key performance indicators for automated transaction monitoring, are multi-interpretable concepts, and the team tasked with optimizing the system's analytical performance must decide which measurement(s) they will use as their key metric (Chau *et al.*, 2020, p. 30).

A high proportion of false positives suggests overreporting. This is a worry for the AML reporting chain, from financial institutions to FIUs, since too many false warnings can jam the system and divert resources from more pertinent investigations. There is a significant operational and cost-efficiency incentive for financial institutions to maintain a low false positive ratio and a high true positive ratio. A major indicator of system quality is the detection rate: how many alarms are generated? However, this detection rate must constantly be weighed against the genuine positive and false positive rates. A high detection rate is meaningless if the real positive alerts remain needles in a haystack of false positives. Currently, a false positive rate of 90 percent, indicating that just one in ten warnings is regarded for further examination, is deemed acceptable and within the risk tolerance of many financial firms and regulators (Chau *et al.*, 2020, p. 30).

The definition of money laundering is a persistent issue for policymakers and AML system designers. Because there is no unique pattern that indicates fraud, money laundering and lawful transactions are frequently mistaken. Constantly shifting fraud trends make it difficult for rule-based systems and policies to stay up. These challenges force organizations to choose between the efficacy and efficiency of their AML system. A system that rapidly identifies fraud requires fewer human analysts and has a greater risk of overlooking fraudulent transactions. A system with a reduced risk is more safe since the majority of transactions will be thoroughly screened; nonetheless, this is expensive for both analysts and the financial institution (Han et al., 2020).

Above-the-line analysis is the process of optimizing the efficiency of analytic systems by examining true or false positives. This appears to indicate that there is also an equivalent below the line. The focus of below-the-line analysis is false negatives. A false negative occurs when the system fails to create an alert when (often in hindsight) the Compliance analyst or investigator would have considered the alert to be a genuine positive in the hypothetical example generated by the system (Chau *et al.*, 2020, p. 30).

In the realm of AML transaction monitoring, technology is used to assist front and back office business activities with a particular business purpose in mind: ensure that it complies with the applicable laws and regulations. Inherently, regulatory developments are the primary driver of these corporate aims. In turn, these regulatory advances are partially driven by the regulatory supervisors' learning process, which is enabled by technical breakthroughs and the rise in analytical capability. The evolution of regulations is also influenced by what regulators and law enforcement witness in the money launderers they target. Technology and the use of (advanced) analytics have the effect of tightening the net, but those who wish to launder money via the system will adapt and thrive as a result. One may certainly talk of an evolution in which the numerous players in this financial and legislative ecosphere respond to one the other's development (Chau *et al.*, 2020, p. 31).

From a technological standpoint, we can identify three areas of knowledge that have contributed to the development of AML transaction monitoring. Data integration, analytics, and data visualization are examples. The development of AML transaction monitoring proceeded along these lines, in this precise sequence. Initially, the problem was how to link to the electronically accessible data and get all the data in one place for the use and analysis of the one particular purpose of AML. Now, the focus is on the analytics applied to that data to refine models and boost alert productivity. In spite of the growing importance of automated alerts, most legal frameworks do not permit a totally automated procedure, and the human element is still regarded as crucial to any AML operation. In order to make sense of the vast amounts of data and the information that may be derived from them, data visualization is gaining ground (Chau *et al.*, 2020, p. 31).

There´s also an educational cycle between the human and computer. Human experience and knowledge produced the rules that taught the computers, it is then with the aid of computers, databases, and electronic data analysis tools that humans learned much more about the data. The new insights are then used to modeling techniques that are ever more intricate and complex. Models are then trained by or with the aid of electronic data, which is frequently enriched by human investigation, and we are gradually moving in the direction of self-learning machines that require minimal human input to further train their own models and increase their own capacity for separating wheat from chaff (Chau *et al.*, 2020, p. 32).

However, the distribution, storage, and processing of financial institutions' data are among the most critical obstacles institutions must overcome while implementing AML. The vast majority of transactions should be accepted in the majority of institutions. Analysts disclose to the authorities any transactions that have been identified as potentially fraudulent. The ultimate determination about whether or not a transaction is actually fraudulent is not always reported to the financial institution. Therefore, financial institutions receive a huge number of questionable transactions, a subset of which are flagged as fraudulent by their analysts but receive no feedback from the authorities regarding the veracity of their decisions. This means that the data that financial institutions can supply to researchers is noisy and frequently lacks a label of "fraudulent" or "legal"; consequently, it is challenging to develop models for predicting fraudulent transactions. In addition, it makes it impossible to evaluate the accuracy of existing approaches by comparing them. Without a true positive and true negative class, it is hard to determine whether a method is effective or whether it outperforms analysts and other approaches. As a result, when building Innovative approaches for AML, it is crucial to consult with analysts, as their feedback may be the sole source accessible for determining the system's performance (Han *et al.*, 2020).

2.1. DETERMINANTS OF RISK IN AML/CFT COMPLIANCE

The risk-based approach [16] encompasses a variety of risk concepts that are applied in transaction monitoring in various ways. Transaction monitoring is ultimately concerned with transaction risk: what is the possibility that this transaction exposes money laundering and, by extension, illegal funds? The risk of the transaction is calculated using algorithms that integrate additional risk concepts (Chau *et al.*, 2020, p. 34).

One of these concepts is the risk represented by the parties to the transaction. If they are internal parties, i.e., customers, then a customer risk level is established, often

[16] Risk-based approach: The Fourth Money Laundering Directive introduces the risk-based approach as a balance between financial crime deterrence and economic stability.

in terms of high, medium, or low. This customer risk may be calculated using a scorecard or determined by an examination of the customer. Obviously, this is not done for all consumers – it would be unrealistic – but for high-value individuals and businesses who are on the verge of high risk, it is not unusual to define an exact risk level. Here comes into play the concepts of Enhanced Due Diligence (EDD) and Special Due Diligence (SDD). However, the majority of customer risk is evaluated based on information collected upon account opening and during the client relationship's lifetime (Chau *et al.*, 2020, p. 35).

The majority of financial institutions analyze the risk of their own products. Frequently, product risk is a distinct type of risk that contributes to customer risk or directly influences the transaction monitoring risk assessment. Purely domestic and common products, such as a standard current or tax-exempt savings account, are deemed to represent a low risk (for money laundering), whereas exotic products with a foreign currency component or those that have historically been favored by money launderers may be assigned a higher risk level (Chau *et al.*, 2020, p. 35).

This takes us to the third risk factor, country risk. The majority of regulatory structures mandate that financial firms evaluate country risk independently. Most, if not all, cross-border financial institutions record risk scores or levels for each nation or region. Occasionally, they are simply copied from a subscription, but bigger financial institutions often have methods to analyze or even compute the risk level for every country and territory in the world. Under the rule-based approach, the non-governmental Financial Action Task Force (FATF) maintained a list of non-cooperative nations and territories, that were incorporated as a blacklist into local rules. The list still remains, although over time, nations on this FATF list have taken steps to enhance their AML regime and have therefore been removed (Chau *et al.*, 2020, p. 35).

Countries may continue to appear on so-called watchlists, alongside persons, companies, and vessels with a registered flag. Possibly, watchlists might be classified as one of the risk factors. They contribute to the client risk, albeit they are often employed during the onboarding of a customer and prohibit accounts from being established for the individual or organisation. In addition, transaction monitoring scenarios often incorporate a variety of rules that precisely examine parties and jurisdictions on watchlists that are engaged in a payment (Chau *et al.*, 2020, p. 35).

Aside from these potentially high-risk aspects of a transaction, there is a distinct concept of transaction risk that relates to the unusualness of the transaction. The basic assumption is that the higher the ML risk, the more uncommon the transaction is for this client or this account. Determining if a transaction is out of the ordinary has become an increasingly complex procedure that incorporates more and more variables. A transaction might be unusual from numerous viewpoints, and the majority of transaction monitoring systems take this into account (Chau *et al.*, 2020, p. 36).

First, there is the perspective of being uncommon relative to the account's usage. Numerous algorithms assess if one or more transactions (suddenly) deviate significantly from the account's use history. One can consider the magnitude of the transaction and the number of transactions in a given period (velocity), but one must also take into consideration more gradual rises or declines in income and spending habits, since they are extremely common. Seasonal changes must be accounted for: many individual consumers and most shops use their accounts more often during the holiday season, while vacation times are characterized by unexpected slumps or surges (Chau *et al.*, 2020, p. 36).

In addition, the account's behavior can be compared to that of similar accounts in order to prevent comparing apples and oranges. Customers with a high net worth will have a dramatically different pattern than those with a midrange or low income. There may be significant differences between the account patterns of manufacturing and retail enterprises. And even within retail, a low-end business in a crowded shopping area will have a completely different revenue and expenditure stream than a high-end retailer in a more exclusive location. Therefore, the majority of financial institutions segment their client base and implement either segment-specific regulations or threshold parameters that vary depending on the threshold. Those financial institutions who go one step further offer the notion of peer groups, in which each client or account is assigned to a group that is anticipated to exhibit similar behavior. A group profile is constructed, either statically or dynamically, and the account's transactions and summary profiles are compared to the group profile. If there is a substantial variance, an alarm will be generated (Chau *et al.*, 2020, p. 36).

As stated previously, the shift from rule-based to risk-based led to a change in responsibility and accountability. In a rule-based system, financial institutions have little responsibility beyond ensuring that the rules are applied. The cost was a deluge of alarms and reports, the most of which were false positives. A risk-based strategy may reduce the number of false positives and the number of reports filed, but at the expense of greater responsibility and the investment in a framework that justifies the (risk) approach selected (Chau *et al.*, 2020, p. 37).

As we have seen, the risk-based strategy broadens the playing field, as there are many permutations of the methodology and uncountable judgments to be taken. The regulatory watchdog may evaluate the robustness of this system at any moment. Financial institutions will be required to justify their transaction monitoring configurations. If country risk is included in the process, it may be necessary to describe explicitly how country risk levels are determined and what is done with this information further down the line. The same holds true for all other risk concepts that comprise the risk-based approach. These techniques and decisions must be documented in a way that explains to a relative outsider (regulatory auditors) how everything functions and demonstrates that it is resilient and fair enough (Chau *et al.*, 2020, p. 37).

In addition, the transition from a rule-based system to a risk-based system has introduced the concept of profiling: to identify if a transaction or pattern of transactions is out of the ordinary, the client must be compared to similar customers. This may quickly backfire; the greater a financial institution's knowledge of a particular client, the greater its understanding of whether or not this consumer can be usefully compared to others (Chau *et al.*, 2020, p. 37).

2.2. WHITE-BOX SYSTEM

Furthermore, a significant amount of mathematical reasoning is included inside the transaction monitoring program. AML accountability cannot be delegated to the software provider; hence, financial institutions will be required to comprehend the program. Financial institutions are permitted to engage regulatory review specialists from the software vendor. However, from the standpoint of regulatory scrutiny, it is always preferable if the solution is white box rather than black box. Typically, black box software conceals the majority or a portion of its internal logic and operations in order to preserve its intellectual property (Chau *et al.*, 2020, p. 50).

This particular concern among other was raised on an unsigned CEO letter to retail banks on common control failings in AML frameworks, published by The Financial Conduct Authority (FCA, 2021a), as can be seen:

> For branches and subsidiaries of overseas firms, we often see group-led transaction monitoring solutions which have not been calibrated appropriately for the business activities and underlying customer base of the UK regulated entity. In these circumstances firms must test whether the system is fit for purpose for the UK entity and where it is not, either tailor the system appropriately, or implement additional risk-based transaction monitoring measures. More broadly, we also find some firms' transaction monitoring systems are based on arbitrary thresholds, often using 'off-the-shelf' calibration provided by the vendor without due consideration of its applicability to the business activities, products or customers of the firm. We often find that firms have difficulty in demonstrating how the thresholds would relate to the levels of expected activity of specific customers or customer cohorts. We also find a lack of understanding of the technical set up of the transaction monitoring systems from those individuals that have responsibility for its operation and effectiveness.

As can be seen, arbitrary thresholds pose a significant concern, the usage of biased data can be a concern, as there are many permutations of the methodology and uncountable judgments to be taken.

Communication with analysts is of the highest significance when creating any AML system, as the final decision is made by the users. Explainable AI approaches function by presenting the user with explicit explanations as to why a prediction was made (e.g., why the system feels a transaction is suspicious) in order to aid the user in making a choice and enhance the user's comprehension of the technology. Any system must be able to explain its decisions in an approachable manner. The European approach emphasizes the necessity for financial institutions to make judgments that are explicable and human-authorized. Any future AML technique must involve a human analyst and guarantee that the analyst correctly comprehends the information supplied to them. Unacceptable is a black-box system that identifies a transaction as "fraudulent" without providing any more context (Han *et al*., 2020).

That's because, recently, the European Union (EU) implemented significant laws (commonly known as GDPR) covering the collection, storage, and use of personal information; these regulations superseded the EU's 1995 Data Protection Directive and went into effect in May 2018. (DPD). Regarding applicability, the new legislation applies universally to industries, EU organizations, and entities that handle EU data. The focus of the data-driven rules is on particular concerns, such as data ownership, transparency, explainability, and the trustworthiness of algorithms that are trained or constructed using such data. In conclusion, GDPR mandates that data-driven automated systems, such as AML systems, must adopt the following throughout implementation: legal data processing and data ownership, explanatory frameworks for the data and algorithms, and ethical compliance (Han *et al*., 2020).

Moreover, in the case of a transaction-monitoring system, when an algorithm predicts an innocent transaction as malicious using metrics that mirror historical data, it is unclear if the boundary between prediction and active avoidance may be utilized to obtain a high true positive rate. When building AI solutions to a particular issue, certain ethical norms must be adhered to in order to manage such situations. In terms of ethics, it is unavoidable that certain human aspects be incorporated into the architecture of the system in order to review and modify the judgments made by the predictive model. Only human evaluators can correct inconsistencies, such as those in the data or (perhaps) a prediction bias due to discriminating features of the data. For instance, when determining whether a transaction is fraudulent or not, an AML system can present its predictions with an explanation to the end user; a final decision is made by the human (who may or may not support the system prediction), and this decision is eventually backpropagated to the system to improve its decision-making capabilities (Han *et al*., 2020).

The significance of human–computer interaction (HCI) is crucial in this setting. Compliance with AML requires the collection of evidence against suspicious transactions. The method is arduous and intricate in practice. For instance, it requires the use of search engines to manually collect and filter data in the operational layer, as well as the study of comparable transactions from a historical repository. Moreover, interactions between a compliance officer and the system are conducted in an effective way. The use of HCI has the potential to bring about considerable advances in this area (Han *et al.*, 2020).

To summarize, the typical AML process in industry consists of a linear pipeline connecting a data source to a rule-based system. The analysts then use their own research to assess if a transaction is real or fraudulent. A certain multistep procedure is followed. AML regimes initially gather and process data. Second, they monitor and screen transactions. A suspicious transaction is identified, and a human analyst determines whether or not the transaction is fraudulent. In general, AML frameworks may be broken down into four tiers. The first layer is the Data Layer, in which relevant data is collected, managed, and stored. This comprises both internal and external data from sources such regulatory bodies, authorities, and watch-lists. The second tier, the Screening and Monitoring Layer, examines clients and transactions for suspicious behaviour. The majority of this layer has been automated by financial organizations into a multi-step process frequently based on rules or risk assessments. If a questionable behavior is discovered, it is forwarded to the Alert and Event Layer for additional review. This procedure involves augmenting the data with past transaction information and supporting documentation in order to examine the flagged transaction. Current AML systems are weak in their use of social media and web content to obtain investigative information. As a result, auditors are limited, which increases the inaccuracy of their judgments and the time necessary to scrutinize each transaction. A human analyst in the Operational Layer decides whether or not to block or authorize a transaction (Han *et al.*, 2020).

In this layer, human agents make the final decision to block, release, or queue a transaction based on the information obtained from the preceding levels. A human agent is required by law to make the ultimate determination regarding a transaction. All transactions are monitored and possible fraudulent transactions are flagged by the previous tiers. Nevertheless, the final choice is made by an individual based on the knowledge supplied by the preceding processes (Han *et al.*, 2020).

In the past ten years, the concepts of artificial intelligence (AI) and machine learning have permeated practically every area of automation, including AML. The improvements might be viewed as ultimately replacing the human element in the processes, i.e. depending only on machines, algorithms, and the software's self-learning capability. They may also be considered as enhancing humans participating in the process by processing data in a way that enables the human worker to focus on the portion of the job that needs judgment. When considering supplementing or even replacing the human element in AML procedures, one must differentiate (at least) two elements of the entire procedure in which humans play a role: the scenario design and optimization process and the triage/investigation phase (Chau *et al.*, 2020, p. 42).

Transaction monitoring cannot be entirely automated to the point where human judgment is completely removed from the equation. A person provides the ultimate judgement for each alert or case, whether productive or nonproductive. The AML analyst, whose duty it is to examine alerts and the data they include, must determine whether to dismiss it as a false positive or to continue researching until a determination is made on whether or not to file a regulatory report (Chau *et al.*, 2020, p. 45).

The human analyst's determination of whether a system-generated alert is genuine or false is the fulcrum upon which the metaphorical arc of transaction monitoring rests. And the same holds true for below-the-line analysis, in which thresholds are regularly decreased to enable the issuance of warnings in situations where they would not have been created with the current settings. These warnings are reviewed by human analysts to ensure that the actual settings do not miss an excessive number of false negatives, i.e., instances that are indicative of money laundering but were not captured by the thresholds (Chau *et al.*, 2020, p. 45).

The human element is of paramount importance in the fight against money laundering. Automated approaches have increased the need for internal investigations that require investigations (Gozman *et al.*, 2018), and because financial service providers must be able to explain to the supervisory authority why they allowed a transaction to proceed, it is unlikely that technology will completely replace the human element. However, it can be expected that not all employees recognize suspicious behavior. AML technologies can be employed in intelligent ways, facilitating the identification, investigation, and prevention of money laundering (Wallhoff, 2020).

Banks and financial service providers employ technologies for transaction monitoring, identifying links between high-risk consumers, identifying criminal networks that may be difficult to locate manually, and for regulatory compliance. However, advanced technology is unlikely to replace the necessary human effort, as financial service providers must be able to explain precisely why a particular transaction was considered non-suspicious. When suspicious transactions occur, technologies can provide alerts, but these notifications must still be reviewed by a person. Nevertheless, technologies are crucial in the fight against money laundering and financial crime (Wallhoff, 2020).

3. UNWANTED ENTAILMENTS OF THE CURRENT SYSTEM

While banks have a significant lot of experience with "pricing" operational and credit risk, the 4th AMLD mandates them to conduct risk assessments in areas where they have no prior experience, especially financial crime. Consequently, financial institutions are required to conduct client due diligence and regular customer surveillance, making them the investigative authorities' extended arm (Sciurba, 2018).

The primary emphasis of anti-money-laundering principles is on safeguarding documentation of financial transactions (the infamous paper trail) and analyzing financial flows critically. The battle against money laundering rests entirely on cooperation between the banking industry and law enforcement. The key to success is mobilizing the professional knowledge and awareness of non-criminal operators. It must be stated that one of the key goals of criminalizing money laundering is to obtain the cooperation of the private sector with law enforcement authorities (Pieth, 1998).

Therefore, we must always keep in mind the following three fundamental concepts that the reporting system entails (Ioannides, 2014, p. 24). Turning private sector stakeholders into secret reporters; transforming financial institutions and enterprises into the eyes of law enforcement and prosecutorial authorities; and transplanting to reporters a sophisticated, qualitative and systemic undercover reporting culture (Ioannides, 2014).

The mandatory rules of financial regulation are highly peculiar, if not socially objectionable, as they stipulate that suspicion can be eliminated only if two specific criteria are met: documentary evidence of the legal sources of the funds involved and the establishment of innocent financial and commercial motives on the part of the parties to the transaction. In summary, when suspects fail to publicly, rationally, and truthfully explain the legal sources of the property they manage, hold, and control, the suspicion of criminal culpability cannot be erased and will thus become the subject of legal proceedings. The imposition of the aforementioned two obligations on natural and legal persons, as any jurist would confirm, not only reveals the confidentiality of financial and commercial transactions, but also consolidates the legal extroversion of two diametrically opposed forces that establish innocence or guilt in the context of anti-money laundering law: the statutorily guaranteed confidential submission of self-induced suspicion by reporters and the publicly offered reasonable and truthful explanations on the part of those who have been reported for alleged wrongdoing (Ioannides, 2014, p. 3).

In light of this, it is essential to recognize that these two opposing forces will vividly depict the suspect's or even the accused's picture of innocence or guilt in the following five phases of money laundering prevention and control: genesis of automated alerts of unusual financial activities; internal processing of the findings of suspicion by financial institutions; submission of Suspicious Activity Reports as disclosures of alleged offences to financial intelligence units (triggering the investigation of the financial affairs of suspects); confidential and compatible with the ECHR financial investigations of suspects; and prosecution of suspects for money laundering, the bringing of the indictment for the offences, and trial (Ioannides, 2014, p. 3).

Transaction monitoring was given a special emphasis because it constitutes itself as the first phase – genesis of automated alerts of unusual activities. As we have seen, the risk-based strategy broadens the playing field, as there are many permutations of the methodology and uncountable judgments to be taken. The regulatory watchdog may evaluate the robustness of this system at any moment. Financial institutions will be required to justify their transaction monitoring configurations. If country risk is included in the process, it may be necessary to describe explicitly how country risk levels are determined and what is done with this information further down the line. The same holds true for all other risk concepts that comprise the risk-based approach. These techniques and decisions must be documented in a way that explains to a relative outsider (regulatory auditors) how everything functions and demonstrates that it is resilient enough (Chau *et al.*, 2020, p. 37).

A human analyst will ultimately examine the generated warnings to evaluate whether the technology appropriately identified the condition. This might be the compliance analyst of the financial institution, his or her colleague or boss, an internal audit team, a regulatory watchdog audit team, or the FIU analysts to whom really suspicious incidents are reported (Chau *et al.*, 2020, p. 29).

A high proportion of false positives suggests overreporting. This is a worry for the AML reporting chain, from financial institutions to FIUs, since too many false warnings can jam the system and divert resources from more pertinent investigations. There is a significant operational and cost-efficiency incentive for financial institutions to maintain a low false positive ratio and a high true positive ratio.

However, financial institutions receive a huge number of questionable transactions, a subset of which are flagged as fraudulent by their analysts but receive no feedback from the authorities regarding the veracity of their decisions. This means that the data that financial institutions can supply to researchers is noisy and frequently lacks a label of "fraudulent" or "legal"; consequently, it is challenging to develop models for predicting fraudulent transactions. In addition, it makes it impossible to evaluate the accuracy of existing approaches by comparing them. Without a true positive and true negative class, it is hard to determine whether a method is effective or whether it outperforms analysts and other approaches. As a result, when building Innovative approaches for AML, it is crucial to consult with analysts, as their feedback may be the sole source accessible for determining the system's performance (Han *et al.*, 2020).

3.1. SUBJECTIVE ANALYSIS

In practice, it is quite troublesome that, in trying to protect themselves, some banks automatically disclose customers at an early stage if there are even the slightest indications of suspicion, even if there is no actual evidence of crime. In the case of R v. gh [2015], 30 [17] the Supreme Court of the United Kingdom raised an additional issue with these legislative excesses, namely that the prosecution offices improperly use charges such as money laundering to significantly expand prosecutorial discretion against those accused of committing crimes. The risk-based approach to financial crime mandated by the 4th AMLD requires banks to evaluate their customers based on factors such as sector risk, occupation risk, type of business risk, geographical and jurisdictional

[17] *R v gh* [2015] 1 wlr 2126.

risk, political risk, distribution/delivery channels risk, product that the customer requires/utilizes risk. And since there are no generally accepted methods for assessing such risk factors, banks are expected to develop their own measures of risk (Sciurba, 2018).

As there are no universally accepted methodologies for evaluating such risk factors, banks are expected to build their own risk measurements. Professor Peter Reuter, co-author of the 2014 report "Global Surveillance of Dirty Money" (Holliday *et al.*, 2014), which evaluates the assessments of regimes to control money laundering and combat terrorism financing, has stated that "the science of risk analysis is poorly developed for money laundering, and it is currently impossible to judge relative risk objectively and systematically." As a result, banks cannot rely on sufficient evidence, but rather on a broad subjective evaluation (Sciurba, 2018).

The Financial Conduct Authority (FCA) published an unsigned CEO letter to retail banks on common control failings in AML frameworks (FCA, 2021a), as stated "Firms often blur responsibilities between the first line business roles and second line compliance roles. We have identified circumstances where compliance departments undertake first line activities, for example completing all due diligence checks or all aspects of customer risk assessment. The implications of this are that first line employees often do not own or fully understand the financial crime risk faced by the firm, impacting their ability to identify and tackle potentially suspicious activity. It also restricts the ability of compliance personnel to independently monitor and test the control framework, which can lead to gaps in the understanding of risk exposure".

Continuing, "A common issue identified through our supervisory work is that Customer risk assessments are often too generic to cover different types of risk exposure which are relevant to different types of relationships. For example, we don't always see firms differentiate between money laundering and terrorist financing risks, or the differing risks presented by a correspondent banking relationship as compared to a customer undertaking trade finance activity" and "We also found that firms confuse the purpose of obtaining SOW (Source of Wealth) and SOF (Source of Origin) information, often requesting, obtaining and verifying the same documents to satisfy these two distinct requirements".

As can be seen from the statement, financial operators often blur responsibilities and do not always understand the risks involved in a particular relationship.

In the UK banks are required to satisfy the conditions imposed by the phrase reasonable grounds for knowing and suspecting, as required by the Poca 2002 the court of the case K v National Westminster Bank [2006][18] ruled that there is no longer a legal requirement for bank employees to have reasonable grounds for knowing that money laundering has occurred; instead, the subjective feeling that it may have occurred is sufficient. Therefore, bank staff are now required to disclose any subjective suspect of money laundering to the authorities (Blair *et al.*, 2021), resulting in a large rise in such reporting in the G20, as can be seen from this graph:

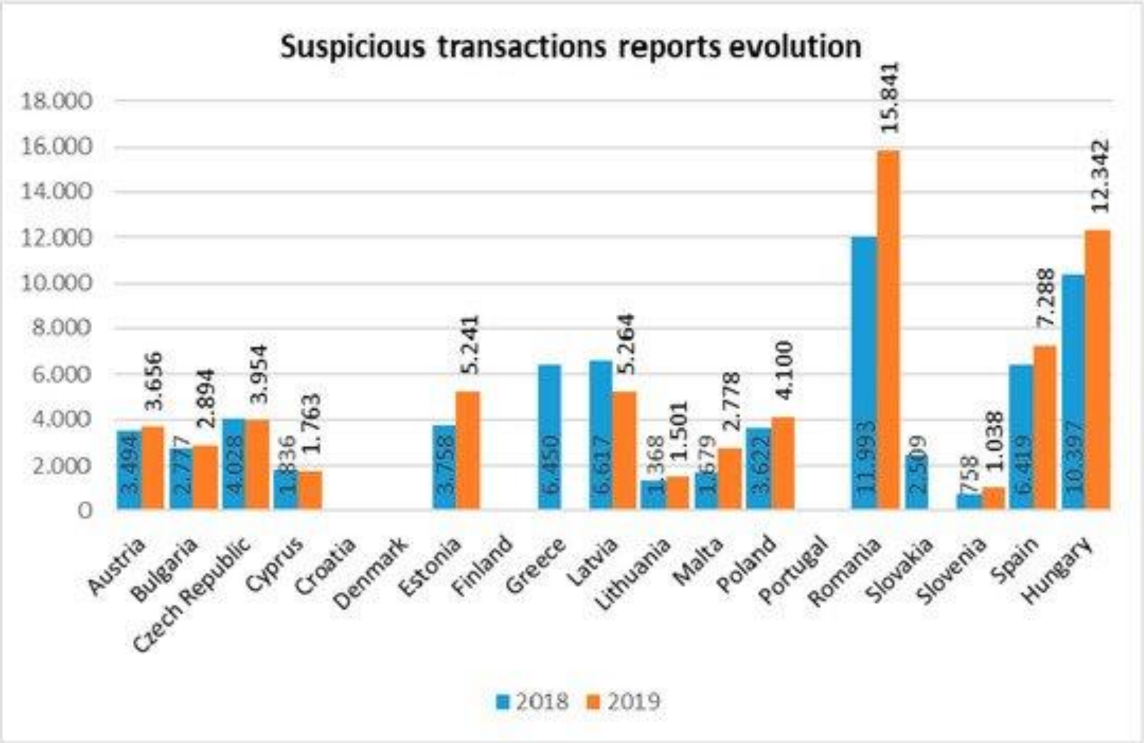

Figure 1. Number of suspicious transactions evolution in the European Member States between 2018–2019. Source: Cotoc *et al.* (2021).

These figures might indicate an erosion of citizens' rights and the principles of the rule of law (Sciurba, 2018). In addition to legal and ethical concerns, regulatory

[18] K Ltd v National Westminster Bank plc (Revenue and Customs Commissioners and Another Intervening) [2006] ewca Civ 1039.

compliance imposes on banks stricter prudential criteria that incur greater expenses. Particularly in environments where banks are under increasing pressure to focus on their core business or are undergoing reorganization, expansion, or high staff turnover, executives are concerned about having the personnel and resources necessary to meet increasingly onerous compliance requirements. This broad drop in risk appetite on the side of banks may result in decisions to terminate client relationships, even with long-standing, problem-free, and ostensibly low-risk consumers and enterprises (Artingstall *et al.*, 2016, p. 16).

3.2. DE-RISKING

Although the establishment of AML and CTF standards in the financial sector is intended to combat money laundering and terrorism financing through early detection, the de-risking attitude of many banks and financial institutions may have reduced the transparency of financial flows (Keatinge, 2014). De-risking is a broad phenomena in which an organization attempts to decrease its exposure to risk by discontinuing operations en masse rather than on an individual basis. For instance, a global corporation may reduce risk by terminating all operations in the Middle East. It would not be called de-risking if the organization reviewed each of its activities individually and ceased those it deemed to exceed a certain risk threshold, even if many of these operations occurred in the same location or industry (Keatinge, 2014).

Occasionally the term "de-risking" is used in this manner, and sometimes in a broader meaning, to refer to the process of minimizing exposure to risk. In order to minimize misunderstanding between "good" and "poor" de-risking, we utilize the more narrow meaning of "de-risking." De-banking happens when a bank unilaterally shuts a person or company's account. This may occur as a result of risk reduction. The comments of compliance offices and banks themselves indicate that regulatory and reputational risk concerns from AML/CFT and sanctions compliance have played a significant impact in the decisions made by banks (Center for Global Development [CDC], 2015, p. 12).

In October 2014, FATF spoke out against wholesale de-risking, arguing that risks should be assessed on a "case-by-case basis." (FATF, 2014). In April of the same year, the FCA issued a similar statement in which it said it will also consider consumer protection and competitiveness considerations in future AML legislation. Following rumors of imminent account closure in Trinidad and Tobago, the Central Bank there issued fresh instructions to banks ordering them to analyze AML/CFT risk on a client-by-client basis, rather than depending on de-risking on a global scale (CDC, 2015, p. 12). However, in a statement last updated on 16/08/21, the FCA recognizes that "We are aware that some banks are no longer offering financial services to entire categories of customers that they associate with higher money-laundering risk" (FCA, 2021b).

Access to the official financial system is difficult for entire groups of clients, even some who are very compliant. Domestic authorities find it challenging to assess risk, create appropriate risk mitigation measures, and inexpensively reduce the AML/CFT risks provided by clients with a higher risk profile while also remaining socially beneficial. FATF has continuously improved and clarified the risk-based strategy; nevertheless, as detailed in sections 1 through 4, these signals are not being effectively communicated to banks, and de-risking continues. This may be due to the fact that FATF has not completely explained some ideas and has not fully implemented certain components of the risk-based strategy (CDC, 2015, p. 12).

In addition, the transition from a rule-based system to a risk-based system has introduced the concept of profiling: to identify if a transaction or pattern of transactions is out of the ordinary, the client must be compared to similar customers. This may quickly backfire; the greater a financial institution's knowledge of a particular client, the greater its understanding of whether or not this consumer can be usefully compared to others (Chau *et al.*, 2020, p. 37).

3.3. PEPs, NGOs AND NON-NATIONALS

In the summer of 2014, the Cordoba Foundation, a UK-based think tank, was given two months to find a new retail bank because its account with HSBC would be cancelled. The rationale provided by HSBC was that "providing financial services...

currently exceeds our risk appetite." (The Cordoba Foundation, 2014). This is an extreme type of de-risking: the removal of financial services, sometimes known as "de-banking." This de-banking occurred despite the fact that the Cordoba Foundation has received funds from the UK government's Prevent program, which tries to prevent extremism. In addition, the Cordoba Foundation is precisely the sort of "expressive NGO" that FATF's categorization suggests is unlikely to be targeted for terrorist exploitation.

This trend is primarily driven by an increase in pressure on banks and financial institutions as a result of the liabilities and penalties associated with AML breaches (CGD, 2015, p. 12). Any application of the risk factors listed above (such as high risk sectors or countries) to a particular relationship would seem to require a generic approach, despite the fact that banking associations and authorities insist that regulatory standards must be applied on an individual basis rather than to entire groups or populations of customers. Such a comprehensive strategy is unquestionably necessary in the case of politically exposed people (PEP) (Sciurba, 2018).

The 4th amld significantly broadens the definition of this group to include family members and other connected parties in addition to requiring banks to do a risk assessment of peps. For all practical purposes, it appears to be a violation of fundamental legal protections to require that family members and individuals connected to peps be scrutinized without any suspicion of wrongdoing and to treat everyone with pep status as a high risk in the absence of proof of financial crime. The instance of pep status serves as an example of the general rule that, if a client is determined to be outside the bank's risk appetite, it will be very difficult to demonstrate that they actually represent a reduced risk; in other words, it is an attempt to demonstrate the opposite (Sciurba, 2018). Many banks and financial institutions have taken preventive action to comply with aml and ctf requirements by classifying entire client groups, such as PEPs and non-nationals, as high risk candidates in order to avoid the possibility of financial consequences (AML Expert, 2016, p. 68). Even seemingly innocent behaviors might put a person at high risk. For instance, the usage of overseas ATMs alone may be enough to close a customer's bank account if they often go abroad or transfer money to nations that are not FATF members (CGD, 2015, p. 12).

The de-risking of high risk customers such as NPOs, PEPs and non-nationals ultimately increase risks to the financial system, as entire sectors (and potentially transactions associated with large regions of the world) may fall out of the regulatory and law enforcement community's view. This impact threatens to "bury" innocent personal and business interactions, limiting transparency. To what degree this influence may be assessed under the existing FATF framework is uncertain. FATF has acknowledged that financial inclusion and anti-money laundering are "complementary policy objectives" and has stated, for instance, that "financial exclusion can potentially pose a significant threat to the successful implementation [of the 40 recommendations] (FATF, 2012). Clearly, authorities have no interest in the loss of transparency, including the rupture of simple bilateral correspondent banking relationships. What has been lacking to date is an AML/CFT plan to prevent this unpleasant consequence (CGD, 2015, p. 12).

Ultimately, the necessity that banks conduct risk assessments for financial crimes such as money laundering and counter-terrorism funding imposes a significant regulatory and compliance burden on banks and can jeopardize their customer relationships (and responsibilities). As financial institutions bear the expense of enforcing AML and CTF regulations, there is little motivation for banks to scrutinize consumers individually, which may result in denial or elimination of accounts for low-income, less lucrative customers (Sciurba, 2018). Banks with a risk-averse approach to compliance, whether out of concerns about their capacity to respond to regulatory or compliance requirements or out of fear of sanctions and penalties for failing to do so, may find it convenient to close the accounts of customers who pose little risk of engaging in financial crimes. In this regard, the aml red flag suggestions for "suspect" consumers based on national origin can be discriminatory and improper. Under the pretense of complying with regulatory obligations, banks might eliminate non-profitable clients. In consequence, the establishment of risk categories may encourage the discrimination of entire groups of individuals, such as those from geopolitically crucial nations. Consequently, the banking clients most likely to be damaged by preemptive enforcement may also be the least integrated into a nation's financial system (Sciurba, 2018).

3.4. FINANCIAL INTEGRATION

In the European Union today, integration into society requires integration into the financial system, including a functioning bank account. Therefore, despite the fact that banks are for-profit businesses and not charities, they still have a social responsibility in addition to their economic function. In order to implement the growing number of AML and CTF rules, institutions have had to develop their own procedures for risk evaluation. In order to comply with regulatory compliance standards, they have formed risk pools based on a general suspicion of certain client categories (Sciurba, 2018). Due to the exorbitant cost of assessing members of these groups individually, impacted customers can be dismissed without justification (Artingstall *et al.*, 2016, p. 16).

The premeditated exclusion of high-risk customers, including PEPs, and non-nationals, constitutes discrimination and violates Article 14 of the ECHR, which prohibits "discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status." (Meyer-Ladewig, 2011).[19] The fundamental problem, then, is no longer just the relationship between a bank and a specific customer, or private contractual obligations; it also involves the systematic exclusion of some groups of people, frequently immigrants or foreigners, which is prohibited by Article 21 of the European Union's Charter of Fundamental Rights' anti-discrimination provisions (European Union, 2012).[20] The Charter of Fundamental Rights became EU primary law on December 1, 2012, when it was incorporated into the Lisbon Treaty. Article 19 TFEU serves as the foundation for the basic right in Article 21(1) of the Charter, while the Explanatory Memorandum to the EU Charter of Fundamental Rights lists Article 14 echr as a source of fundamental legal principle. As opposed to Article 14 of the European Convention on Human Rights, Article 21 of the Charter provides non-discrimination with regard to all rights, including non-discrimination based on personal characteristics like race, origin, or gender (Sciurba, 2018).

[19] Article 14 of the echr is also implemented in the UK Human Rights Act 1998.

[20] Charter of Fundamental Rights of the European Union [2012] oj c326/391 art. 21.

In light of this, the EU's existing AML legislation may not adhere to the mandatory concept of proportionality because of the possible civil rights restrictions. The general application of suspicious activity criteria to groups of customers on the basis of "know your customer" requirements can be both insufficient and discriminatory. This is because AML and CTF Legislation, in practice, may create economic incentives that drive banks to adopt policies that exclude entire customer groups rather than bear the cost of examining suspected violations on a case-by-case basis. The bank's automated access to client data and information sharing could be turned it into a subjective, increasingly arbitrary preventive system. Banks are under pressure to take proactive measures to identify and flag "suspect" clients as collaborators with law enforcement. In an effort to reduce bank liability, preventative actions to build de-risking policies can led to risk pools that prevent many trustworthy clients from creating accounts or result in the termination of an existing account (Sciurba, 2018).

In practice, these unintended effects of the AML and CTF laws result in the exclusion of growing numbers of people from the banking system by discriminating against entire groups based on personal characteristics, such as being a resident foreigner, in violation of Articles 14 in connection with Article 8 of the European Convention on Human Rights and Article 21 of the Charter of Fundamental Rights of the European Union (Meyer-Ladewig, 2011, p. 287).[21] The European Court of Justice has not issued enough decisions pertaining to Article 21 of the Charter since it was incorporated into the Lisbon Treaty in 2012, which would have adequately governed the formal and substantive requirements for its application and interpretation. The obligations of the legislator, the principles of proportionality and legal certainty, and the sufficient justification for unequal treatment under some AML regulations, however, are not clear under the current AML legislation. As a result, the investigative authorities abdicate their responsibility and place onerous regulatory requirements on banks, who are forced to monitor financial crime without the resources and knowledge

[21] The ECHR requires that the justification in case of difference of treatment merely due to nationality must provide particularly important grounds of justification. Here, see European Court of Human Rights (ECHR) judgement in the case of Gaygusuz v Austria (16 September 1996).

of law enforcement agencies. This is because there is no precise regulation on how to implement individual KYC requirements. Therefore, in order to save expenses and avoid potential liability, financial institutions can implement a de-risking program that primarily denies consumers access to their accounts and closes (or prevents the opening of) accounts for those who appear to be less profitable (Sciurba, 2018).

3.5. PROPORTIONALITY

The mandatory rules of financial regulation are highly peculiar, if not socially objectionable, because they stipulate that suspicion can be eliminated only if two specific criteria are met: documentary evidence of the legal sources of the funds involved and innocent financial and commercial motives on the part of the transaction parties. When suspects fail to publicly, rationally, and truthfully explain the lawful origins of the property they manage, own, and control, criminal guilt is suspected and legal processes ensue. Any lawyer would agree that imposing the aforementioned two obligations on natural and legal persons exposes the secrecy of financial and business interactions and consolidates the legal extroversion of two diametrically opposed forces that determine guilt or innocence in the context of anti-money laundering law: the statutorily guaranteed confidentiality submission of self-induced suspicion by reporters and the offered justification by the accused part (Ioannides, 2014, p. 3).

We must move further down the path of devolving responsibility for risk assessment to the national and institutional level, replacing the requirement for enhanced due diligence in specific cases with a requirement for due diligence directly correlated with the level of risk identified by the relevant risk assessment. Risk evaluations of nonprofits should be based on the functional structure of the organization and its operations, not its legal status. Specifically, it must be made obvious that these entities have distinct risk profiles based on their operations and risk detection and mitigation procedures. The same goes to PEPs and non-nationals, the equirement for due diligence must be directly correlated with the level of risk identified by the relevant risk assessment, not only because of their high-risk status.

A holistic approach is required, as an alert is generated, in case of suspicion, the financial operator must not only inquire about the identity and basic risk factors of the parties involved but also about the economic motivations for the transaction. Oftentimes, identification and basic risk assessment, such as a risk scorecard are insufficient; only when financial operators are required to match their information on transactions with data on the client and sometimes even their knowledge of the client's performance over a period of time can suspicious structures become evident. Without this requirement, it will be a matter of chance whether a transaction is actually deemed suspicious (Pieth, 1998).

CONCLUSION

The goal of the current thesis was to investigate the battle against terrorism financing and money laundering in the context of the existing European framework, as well as some of its unintended repercussions.

The first chapter elucidated some basic aspects of money laundering and the stages involved in the process. Further on, the research took place analyzing the global importance of money laundering prevention, along with the role of the FATF, and how all of that enables and validates the use of technologies, such as transaction monitoring, for combating the issue within the European framework. A comprehensive elucidation of the reporting system and its entailments was the key objective for the initial chapter.

Transaction monitoring was given a special emphasis because it constitutes itself as the first phase – genesis of automated alerts of unusual activities; it is also the technology current applied in firms within the EU and because it illustrates the human analysis throughout the whole process.

The need for transparency in given system was also highlighted. The third chapter elucidated the incongruity of two seemly public interest matters ML-FT prevention and its negative reflections in consumer protection and financial integration.

The complexity of the theme was also noted throughout the thesis, given by the vast entanglements of the reporting system, the innumerous recommendations proposed by dedicated agencies, the constant law amendments and even the technicalities in current technologies.

Regarding transaction monitoring, the mighty origin of a complex reporting scheme (Suspicious Activity Reports – Tactical and Strategic Analysis – Exchange of Information), a technical approach was utilized, especially to illustrate the contingency and prudential costs expected of financial institutions. The determinants of risk factors were also examined.

The GDPR requires that data-driven automated systems, such as AML systems, adopt measures throughout implementation, including legal data processing and data ownership, explanatory frameworks for the data and algorithms, and ethical compliance. In that context, the need for transparency was also appropriately emphasized.

In the other hand, the de-risking approach of some firms could benefit from automated systems that precisely utilize and arrange customer's data in categories, possibly ostracizing low-profit costumers. All of this concealed under the pretense of ML/FT prevention.

Even if that's not the case for all firms - given the pressure emitted by dedicated agencies - and the case-by-case approach is thoroughly utilized, we still need to consider that human-judgement is always present, we could be looking for some biased-driven decisions and discrimination, be it in data analysis or in investigative measures – especially in a context of financial crime red flags and pre-defined risk scores. For this reason, the requirement for due diligence ought to be directly correlated with the level of risk identified by the relevant risk assessment, as innumerous factors are to be taken in regard.

As an alert is created, the financial operator must take a comprehensive approach and not only enquire about the parties' identities and the key risk characteristics associated with them, but also about the economic aspects behind the transaction.

Identification and basic risk assessment are frequently insufficient, suspicious structures only become apparent when financial operators are required to compare their information on transactions with information on their clients, and occasionally even with their knowledge of the client's performance over time. Nonetheless, in the absence of this criteria, it will be up to chance whether a transaction is truly regarded as suspicious.

The concern on PEPs, NGOs and non-nationals was more prominent given the apparent vulnerability of such deemed high-risk customers, however, any citizen of the EU might be accused of financial crime.

We also need to consider that 90% of alerts generated are false (given the prescribed risk acceptance), hence, the number of customers scrutinized and reports submitted ought to grow exponentially and indefinitely – along with its associated costs. It is relevant to note that state austerity policies and legislative omissions also exacerbated this tendency. At the end of the day, we are talking about the vigilance of millions of European citizens.

Furthermore, firms are not always informed of the final decision about whether a transaction is indeed fraudulent. As a result, financial institutions receive a sizable volume of dubious transactions, a portion of which are labeled as fraudulent by their analysts but do not obtain confirmation from the authorities that their judgments were correct.

The exchange of information - an essential element of a successful reporting system – is missing here. The deflection of responsibility is prominent. Financial institutions are required to develop their own risk measurements whilst not being informed if the work developed is appropriate. A great deal of subjective reasoning is expected.

To conclude, the same self-interest that pushes individuals to financial crime, can also be seen in de-risking measures applied in some financial institutions, all of this in a context of State's austerity policies and legislative omissions.

REFERENCES

AML EXPERT - **Anti Money Laundering Exam Study Guide & Practice Exam**. 1st ed. California: Create Space Independent Publishing Platform, 2016.

ARTINGSTALL, D. [et al.] - **Drivers & Impacts of Derisking: A study of Representative Views and Data in the UK**. Guildford: John Howell & Co. Ltd. for the Financial Conduct Authority, 2016.

BERGER, A. N. [et al.] - Bank concentration and competition: An evolution in the making. **Journal of Money, Credit, and Banking**. 36: 3 (2004) 433-451.

BLAIR, W.; BRENT, R.; GRANT, T. - **Banks and Financial Crime. The International Law of Tainted Money**. 2nd ed. Oxford: Oxford University Press, 2017.

BLANCO CORDERO, I. - Negocios socialmente adecuados y delito de blanqueo de capitals. **Anuario de Derecho Penal y Ciencias Penales**. Tomo L, fascículo único, enero-diciembre (1997) 263-291.

BLANCO CORDERO, I. - El delito fiscal como actividad delictiva previa del blanqueo de capitals, **Revista Electrónica de Ciencia Penal y Criminología**. 13:01 (2011), 1-46.

BLANCO CORDERO, I. - **El delito de blanqueo de capitales**. 3rd Edition. Cizur Menor: Aranzadi, 2012.

CENTER FOR GLOBAL DEVELOPMENT - **Unintended Consequences of Anti-Money Laundering Policies for Poor Countries: a cgd Working Group Report**. Washington, DC: CGD, 2015. [Accessed 30 Jul. 2022]. Available at www.cgdev.org/sites/default/files/CGD-WG-Report-Unintended-Consequences-AML-Policies-2015 .pdf

CHAU, D.; NEMCSIK, M. V. D. - **Anti-Money Laundering Transaction Monitoring Systems Implementation: Finding Anomalies.** 1st ed. New York: Wiley (Wiley and SAS Business Series), 2020.

CHINCHILLA, A. - Blanqueo de dinero. In GÓMEZ, Avilés – **El Enriquecimiento Ilícito**. Alicante: Editorial Club Universitario, 2011. p. 133-157.

CHOO, H. C. [et al.]. - Anti- Money Laundering and its Effectiveness. **Malaysian Accounting Review**. 13:2 (2014) 109-124.

CLOUGH, J. - **Principles of Cybercrime**. Cambridge: Cambridge University Press, 2010.

COLLADO MEDINA, J. - El blanqueo de capitales: una aproximación. In COLLADO MEDINA, J. (Coord.) - **La investigacio´n criminal y sus consecuencias jurídicas**. Madrid: Dykinson, 2010. p. 469-491.

COTOC, C.-N. [et al.] - Efficiency of Money Laundering Countermeasures: Case Studies from European Union Member States. **Risks**. 9:6 (2021), 120. https://doi.org/10.3390/risks9060120.

COSTANZO, P. - The risk-based approach to anti-money laundering and counter- terrorist financing in international and EU standards: what it is, what it entails. In UNGER, Brigitte; VAN DER LINDE, Daan - **Research handbook on money laundering**. Cheltenham: Edward Elgar Publishing, 2013.

COX, D. - **Handbook of anti-money laundering**. New York: John Wiley & Sons, 2014.

DE MEULEMEESTER, J. L.; ROCHAT, D. - A causality analysis of the link between higher education and economic development. **Economics of Education Review**. 14:4 (1995) 351- 361.

DEMETIS, D. S. - **Technology and anti-money laundering: A systems theory and risk- based approach.** Cheltenham: Edward Elgar Publishing, 2010.

DIAMOND, L. - Democracy in Decline: How Washington Can Reverse the Tide. **Foreign Affairs** [In line]. Jul./Aug (2016).

EUROPEAN COMMISSION - **Consultations: Internal Market, Call for Evidence: Review of Directive 2003/6/EC on Insider Dealing and Market Manipulation 4/09'**. Brussels: European Commission, 2009 [Accessed 28 Apr. 2022]. Available at http://europa.eu/internal_market/consultations/docs/2009/market_abuse/call_for_evidence .pdf.

EUROPEAN COMMISSION - **Proposal for a Directive of the European Parliament and of the Council on the freezing and confiscation of proceeds of crime in the European Union' COM (2012) 85 final**. Brussels: European Commission, 2012. https://op.europa.eu/en/publication-detail/-/publication/9428a53e-684f-4788-a569-96cd78abe533/language-en/format-PDF

EUROPEAN COURT OF HUMAN RIGHTS - **Case of Gaygusuz v Austria (16 September 1996)**. Strasbourg: ECHR, 1996. [Accessed 30 July 2022]. Available at http://hudoc.echr.coe.int/eng?i=001-58060.

EUROPEAN UNION - **Corporate and Financial Malpractice**. Brussels: European Union, 2006. [Accessed 28 Ap. 2022]. Available at https://op.europa.eu/en/publication-detail/-/publication/0dd5e872-2ea9-4810-80ee-17531427ad8b/language-en/format-XHTML

EUROPEAN UNION - **Mutual Administrative Assistance in the Fight against Fraud**. Brussels: European Union, 2007. [Accessed 28 Ap. 2022]. Available at http://Europa.eu/scadplus/leg/en/lvb/110122.htm

EUROPEAN UNION - **European Union Committee, Money Laundering and the Financing of Terrorism (HL 2008–09, 132–I)**. Brussels: European Union, 2008a. [Accessed 28 Ap. 2022]. Available at <http://www.publications.parliament.uk/pa/Id200809/Id select/Ideucom/132/13204.htm#a2> accessed 28 April 2022.

EUROPEAN UNION - **Minutes of Evidence, Money Laundering and the Financing of Terrorism (HL 2008–09, 132–II). Question 463 of Lord Dear addressed to witness Mr Ian Pearson, Member of the House of Commons, Economic Secretary to the Treasury.** Brussels: European Union, 2008b. [Accessed 28 Ap. 2022]. Available at http://www.publications.parliament.uk/pa/Idselect/Ideucom/132/9042904.htm

EUROPEAN UNION - **Europa, 'Fiscalis 2013 (2008–2013)**. Brussels: European Union, 2008c. [Accessed 28 Ap. 2022]. Available at http://europa.eu/scad plus/leg/en/lvb/111051.html

EUROPEAN UNION - **Charter of Fundamental Rights of the European Union [2012] oj c326/391 art. 21**. Brussels: European Union, 2012.

EUROPOL - **Financial & Property Crimes 1/06'**. Hague: Europol, 2006. [Accessed 15 April 2022]. Available at http:// www.Europol.europa.eu/publications/Serious_Crime_Overviews/ overviewFCP.pdf.

FATF - Report of 6 February (FATF-I). In Gilmore, W.C. (ed.) - **International Efforts to Combat Money Laundering**. Cambridge: Grotius Publications, 1990, Chapter I, Document B, p. 4-24.

FATF - **Risk-Based Approach Guidance for Casinos**. Paris: FAFT, 2008a. Available at www.fatf-gafi.org

FATF - **Risk-Based Approach Guidance for Real Estate Agents**. Paris: FAFT, 2008b. Available at www. fatf-gafi.org

FATF - **Report, Money Laundering Through the Football Sector**. Paris: FAFT, 2009a. Available at www. fatf-gafi.org

FATF - **Report, Risk-Based Approach Guidance for the Life Insurance Sector**. Paris: FAFT, 2009b. [Accessed December 2012]. Available at www.fatf-gafi.org

FATF - **Report, Vulnerabilities of Casinos and Gaming Sector**. Paris: FAFT, 2009c. [Accessed Dec. 2012]. Available at www. fatf-gafi.org

FATF - **Report, Money Laundering Using Trust and Company Service Providers**. Paris: FAFT, 2010a Available at www.fatf-gafi.org

FATF - **Report, Money Laundering Through Money Remittance and Currency Exchange Providers**. Paris: FAFT, 2010b. Available at www.fatf-gafi.org

FATF - **Annual Report 2010-2011**. Paris: FAFT, 2011a. [Accessed Dec. 2012]. Available at www.fatf-gafi.org

FATF - **Report, Laundering the Proceeds of Corruption**. Paris: FAFT, 2011b. [Accessed Dec. 2012]. Available at www.fatf-gafi. org

FATF - **Report, Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants**. Paris: FAFT, 2011c. [Accessed Dec. 2012]. Available at www.fatf.gafi.org

FATF - **Report, Organised Maritime Piracy and Related Kidnapping for Ransom**. Paris: FAFT, 2011d. [Accessed Dec. 2012]. Available at www.fatf-gafi.org

FATF - **Declaration of the Ministers and Representatives of the Financial Action Task Force**. Paris: FAFT, 2012.

FATF - **FATF clarifies risk-based approach: case by case, not wholesale de-risking**. Paris: FAFT, 2014.

FATF - **FATF Report to G20 Finance Ministers and Central Bank Governors**. Paris: FAFT, 2018. [Accessed Jan. 2019]. Available at https://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf

FATF - **INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION The FATF Recommendations**. Paris: FAFT, 2022. Available at https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

FERRO VEIGA, J. M. - **Aspectos legales sobre el delito fiscal, la investigacio´n patrimonial y el blanqueo de capital: radiografı´a de las tramas y de la delincuencia organizada nacional y transnacional**. Alicante: Editorial Club Universitario, 2011.

FINANCIAL CONDUCT AUTHORITY - **Unsigned copy of a Dear CEO letter sent to Retail Banks (only) on 22 May 2021**. London: FCA, 2021a. Available at https://www.google.com/search?q=Unsigned+copy+of+a+Dear+CEO+letter+sent+to+Retail+Banks+(only)+on+22+May+2021.&oq=Unsigned+copy+of+a+Dear+CEO+letter+sent+to+Retail+Banks+(only)+on+22+May+2021.&aqs=chrome..69i57.156j0j7&sourceid=chrome&ie=UTF-8#:~:text=Dear%20CEO%20Letter%20Common,%E2%80%BA%20 correspondence%20%E2%80%BA%20dear%2Dceo

FINANCIAL CONDUCT AUTHORITY - **De-risking: managing money-laundering risk**. London: FCA. 2021b Available at https://www.fca.org.uk/firms/money-laundering/derisking-managing-risk

GAO, S.; XU, D. - Conceptual modeling and development of an intelligent agent- assisted decision support system for anti-money laundering. **Expert Systems with Applications**. 36:2 (2009) 1493-1504.

GEIGER, H.; WUENSCH, O. - The fight against money laundering: An economic analysis of a cost-benefit paradoxon. **Journal of Money Laundering Control**. 10:1 (2007) 91-105.

GILL, M.; TAYLOR, G. - Preventing money laundering or obstructing business? Financial companies' perspectives on 'know your customer'procedures. **British Journal of Criminology**. 44:4 (2004) 582-594.

GOZMAN, D.; CURIE, W.; & SEDDON, J. - Catching the Banksters: The Use of Big Data Analytics in Billion Dollar Regulatory Investigations. **Proceedings of the 51st Hawaii International Conference on System Sciences**. (2018). Available at http://www.lusem.lu.se/library

HAFFKE, Lars [et al.] - Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them. **Journal of Banking Regulation**. 21:2 (2020) 125-138. Available at http://dx.doi.org/10.2139/ssrn.3328064

HAFFKE, Lars; FROMBERGER, Mathias; ZIMMERMANN, Patrick - Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them (February 3, 2019). **Journal of Banking Regulation**. 21:2 (2020) 125-138. Available at https://ssrn.com/abstract=3328064 or http://dx.doi.org/10.2139/ssrn.3328064

HAN, Jingguang [et al.] - Artificial Intelligence for Anti-Money Laundering - A Review and Extension. **Digital Finance**. 2 (2020) 211–239. Available at https://ssrn.com/abstract=3625415

HER MAJESTY'S TREASURY - **The Financial Challenge to Crime and Terrorism 02/2007**. London: HM Treasury, 2007. [Accessed 28 Apr. 2022]. Available at http://www.hm-treasury.gov.uk/d/financialchallenge_crime_280208.pdf.

HEINEMAN JR, B. W.; HEIMANN, F. - The long war against corruption. **Foreign Affairs**. (2006) 75-86.

HINTERSEER, Kris - Criminal Finance: The Political Economy of Money Laundering in a Comparative Legal Context. In RIDER, Barry (ed.) - **Studies in Comparative Corporate and Financial Law**. London, University of London, 2002

HM TREASURY AND HOME OFFICE - **National risk assessment of money laundering and terrorist financing 2017**. London: UK Government, 2017. [Accessed 21 Jan. 2019]. Available at www. assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf

HOLLIDAY, R. C.; LEVI, M.; REUTER, P. - **Global Surveillance of Dirty Money: Assessing Assess- ments of Regimes to Control Money Laundering and Combat the Financing of Terrorism**. California: Center on Law and Globalization, 2014.

HOUBEN, R.; STEVENS, A. - **Cryptocurrencies and Blockchain – Legal context and implications for financial crime, money laundering and tax evasion**. Brussels, BE: Policy Department for Economic, Scientific and Quality of Life Policies, 2018. [Accessed on 04 may 2022]. Available at www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

HUGEL, P.; KELLY, J. - Internet gambling, credit cards and money laundering. **Journal of Money Laundering Control**. 6:3 (2002) 57-65.

IMF - **The IMF And The Fight Against Money Laundering And The Financing Of Terrorism. A Fact Sheet**. Washington: IMF, 2004.

IOANNIDES, Emmanuel - **Fundamental Principles of EU Law Against Money Laundering**. Farnham: Ashgate Pub Co, 2014.

JURADO, N.; GARCÍA, R. - **El blanqueo de capitales: Globalización financiera, economía sumergida y blanqueo de capitales**. Chisinau: Editorial Academica Espanola, 2011.

KEATINGE, Tom - Breaking the Banks: The Financial Consequences of Counterterrorism. **Foreign Affairs.** June 26 (2014). [Accessed 30 July 2022]. Available at https://www.foreignaffairs.com/articles/united-states/2014 -06-26/breaking-banks

KEATINGE, Tom [et al.] - **Virtual currencies and terrorist financing: assessing the risks and evaluating responses**. Brussels, BE: Policy Department for Citizen's Rights and Constitutional Affairs, 2018. [Accessed 21 Jan. 2019]. Available at www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf

KNORZ, J. - **Der Unrechtsgehalt Des 261 Stgb**. Frankfurt: Peter Lang, Europaischer Verlag der Wissenschaften, 1996.

KRUSS, G. [et al.] - Higher education and economic development: The importance of building technological capabilities. **International Journal of Educational Development**. 43 (2015) 22-31.

KSENIA, G. - Can corruption and economic crime be controlled in developing countries and if so, is it cost-effective?. **Journal of Financial Crime**. 15:2 (2008) 223- 233.

LAVORGNA, A. - Organised crime goes online: realities and challenges. **Journal of Money Laundering Control**. 18:2 (2015), 153-168.

MASCIANDARO, D. - Money laundering: the economics of regulation. **European Journal of Law and Economics**. 7:3 (1999) 225-240.

MASCIANDARO, D. - Financial supervisory unification and financial intelligence units. **Journal of Money Laundering Control**. 8:4 (2005) 354-370.

MEKPOR, Emmanuel Senanu [et al.] - The determinants of anti-money laundering compliance among the Financial Action Task Force (FATF) member states. **Journal of Financial Regulation and Compliance**. 26:3 (2018), 442-459. Available at https:// doi.org/10.1108/JFRC-11-2017-0103

MERRITT, C. - Mobile money transfer services: the next phase in the evolution of person-to-person payments. **Journal of Payments Strategy & Systems**. 5:2 (2011) 143-160.

MEYER-LADEWIG, Jens - **Emrk. Europäische Menschenrechtskonvention. Handkommentar**. 3rd ed. Baden-Baden: Nomos, 2011.

MILLS, J. - Internet casinos: a sure bet for money laundering. **Journal of Financial Crimen**. 8:4 (2001) 365-383.

NAHEEM, M. A. - Money laundering using investment companies. **Journal of Money Laundering Control.** 18:4 (2015) 438-446.

NAYLOR, R. T. - **Hot Money and the Politics of Debt**. 1st ed. London: Unwin Hyman Limited, 1987.

NUNEZ PAZ, M. A. - Tipologías criminales de blanqueo. Técnicas de comisión. In SOUTO, Miguel Abel; STEWART, Nielson Sánchez - **II Congreso sobre prevención y represión del blanqueo de dinero (ponencias y conclusiones del congreso internacional celebrado en Barcelona en noviembre de 2010)**, Barcelona, 2011.

OSUJI, E. - Foreign Direct Investment and Economic Growth in Nigeria: Evidence from Bounds Testing and ARDL Models. **Journal of Economics and Sustainable Development**. 6:13 (2015) 205-211.

PICARD, P. M.; PIERETTI, P. - Bank secrecy, illicit money and offshore financial centers. **Journal of public economics**. 95:7 (2011) 942-955.

PIETH, M. - Zur Einfu¨hrung: Geldwa¨scherei und ihre Beka¨mpfung in der Schweiz. In PIETH, M. (Ed.) - **Bekampfung der Geldwascherei: Modellfall Schweiz?**. Basel: Helbing & Lichtenhahn, 1992. p. 1-27.

PIETH, M. - The Prevention of Money Laundering: A Comparative Analysis. **European Journal of Crime, Criminal Law and Criminal Justice**. 6:2 (1998) 159-168. Available at https://doi.org/10.1163/157181798X00166

PUTMAN, R. D. - Diplomacy and Domestic Politics: the Logic of Two-level Games. **International Organization**. 42:3 (1988) 427-460.

PWC - **Anti-Money Laundering: Understanding Global KYC Differences**, 2012. [Assessed 27 Feb. 2017]. Available at www.pwc.co.uk.on

RAWLINGS, G.; UNGER, B. - Competing for criminal money. Discussion **Paper Series/Tjalling C. Koopmans Research Institute**. 5:26 (2005).

RIDER, Barry - **Taking Money Launderers to the Cleaners: Part 1**. PCB 2, 1996a, p. 134–138.

RIDER, Barry - **Taking Money Launderers to the Cleaners: Part 2**. PCB 3, 1996b, p. 201–210.

RIDER, Barry - **Taking Money Launderers to the Cleaners: Part 3.** PCB 4, 1996c, p. 265–272

ROWE, M.; FRANTZ, J.; BOZALEK, V. - The role of blended learning in the clinical education of healthcare students: a systematic review. **Medical Teacher**. 34:4 (2012) e216- e221.

SCHNEIDER, M. F.; ENSTE, D. - **Shadow economies around the world: Size, causes, and consequences (No. 0-26)**. Washington: IMF, 2000.

SCHNEIDER, F. - Money laundering and financial means of organised crime: some preliminary empirical findings. **Global Business and Economics Review**. 10:3 (2008) 309- 330.

SCHNEIDER, F.; WINDISCHBAUER, U. - Money laundering: some facts. **European Journal of Law and Economics**. 26:3 (2008) 387-404.

SCHROEDER, W. R. - Money Laundering: A Global Threat and the International Community=s Response. **FBI Law Enforcement Bulletin**. (2001) 1–7.

SCIURBA, M. - The Heart of Know Your Customer Requirements: The Discriminatory Effect of AML and CTF Policies in Times of Counter-Terrorism in the UK. **European Journal of Crime, Criminal Law and Criminal Justice**. 26:3 (2018) 222-235. Available at https://doi.org/10.1163/15718174-02603003

SHARMAN, J. C. - Power and Discourse in Policy Diffusion: Anti-Money Laundering in Developing States. **International Studies Quarterly**. 52:3 (2008) 635-656.

SHARMAN, J. C.; CHAIKIN, D. - Corruption and Anti-Money-Laundering Systems: Putting a Luxury Good to Work. **Governance**. 22:1 (2009) 27-45.

SHEHU, A. Y. - Should gambling be a predicate for money laundering?. **Journal of Money Laundering Control**. 7:3 (2004) 254-260.

SOUTO, M. Abel - Money laundering, new technologies, FATF and Spanish penal reform. **Journal of Money Laundering Control**. 16:3 (2013) 266-284. Available at https://doi.org/10.1108/JMLC-01-2013-0002

SOUZA, J. D. - **Terrorist Financing, Money Laundering, and Tax Evasion. Examining the Performance of Financial Intelligence Units**. Boca Raton, FL: CRC Press, 2012.

SULLIVAN, K., ed. - What Is Money Laundering?. In **Anti–Money Laundering in a Nutshell. Awareness and Compliance for Financial Personnel and Business Managers**. New York: Apress, 2015, p. 1-13.

TEICHMANN, F. M. J. - Financing terrorism through cryptocurrencies – a danger for Europe?. **Journal of Money Laundering Control**. 21:4 (2018) 513–519.

THE CORDOBA FOUNDATION - **Response to HSBC closure of The Cordoba Foundation bank account**. London: The Cordoba Foundation, 2014. https://thecordobafoundation.com/news/news-press/response-to-hsbc-closure-of-the-cordoba-foundation-bank-account/

THE EGMONT GROUP - **Information Paper of Financial Intelligence Units**. Toronto: The Egmout Group, 2004.

THE EGMONT GROUP - **Benefits of Egmont Group Membership**. Toronto: The Egmout Group, 2009. [Accessed 04 May 2022]. Available at http://www.egmontgroup.org/files/library_egmont_docs/egmont_membership_benefit.pdf.

THOMAS, M. A. - What do the worldwide governance indicators measure?. **The European Journal of Development Research**. 22:1 (2010) 31-54.

TIWARI, M.; GEPP, A.; KUMAR, K. - A Review of Money Laundering Literature: The State of Research in Key Areas. **Pacific Accounting Review**. 32:2 (2020) 271-303. Available at https://doi.org/10.1108/PAR-06-2019-0065

TUPMAN, W. A. - The business of terrorism. In GODDARD, S.; NIKITIN, A.T.; FITUNI, L. I. (eds.) - **Financial Monitoring of Cash Flows Aiming to Prevent the Financing of Terrorism**. Buenos Aires: IIUE Publishing, 2005, p. 112-140.

UNGER, B. - Money Laundering. In **Encyclopedia of Criminology and Criminal Justice**. New York: Springer, 2014, p. 3137-3144.

UNGER, B.; BUSUIOC, E. M. - **The scale and impacts of money laundering**. Cheltenham: Edward Elgar Publishing, 2007.

Unger, B.; Den Hertog, J. -Water always finds its way: Identifying new forms of money laundering. **Crime, Law and Social change**. 5:3 (2012) 287-304.

UNGER, B.; VAN DER LINDE, D., eds. - **Research handbook on money laundering**. Cheltenham: Edward Elgar Publishing, 2013.

UNGER, B.; VAN WAARDEN, F. - How to Dodge Drowning in Data? Rule-and Risk- Based Anti-Money Laundering. **Review of Law and Economics**. 5:2 (2009).

UNGER, B. [et al.] - **The Economic and Legal Effectiveness of the European Union Anti-Money Laundering Policy**. Cheltenham: Edward Elgar Publishing, 2014.

UNODC - **Topics: Definition of Money Laundering**. [Assessed 2nd June 2017]. Nairobi, Kenya: UNODC, 2014. Available at www.undoc.org.

VAN BERGEIJK, P. A.; BRAKMAN, S., eds. - **The gravity model in international trade: Advances and applications**. Cambridge: Cambridge University Press, 2010.

VANDEZANDE, N. - **Virtual Currencies: A Legal Framework**. Cambridge: Intersentia, 2018.

VARESE, F. - How mafias take advantage of globalization. The Russian mafia in Italy. **The British Journal of Criminology. An International Review of Crime and Society**. 52:2 (2012) 235-253.

VERDUGO YEPES, C. - **Compliance with the AML/CFT International Standard: Lessons from a Cross-Country Analysis. IMF Working Paper No. 11/177**. Washington: IMF, 2011.

VERHAGE, A. - **The anti money laundering complex and the compliance industry**. London: Taylor & Francis, 2011.

VIRITHA, B.; MARIAPPAN, V.; VENKATACHALAPATHY, V. - Combating money laundering by the banks in India: compliance and challenges. **Journal of Investment Compliance**. 16:4 (2015) 78-95.

WALKER, J. - **Estimates of the extent of money laundering in and through Australia. Paper prepared for AUSTRAC**. Queanbeyan: John Walker Consulting Services, 1995.

WALKER, J.; UNGER, B. - Measuring global money laundering: the Walker gravity model. **Review of Law and Economics**. 5:2 (2009) 821-853.

WALL, D. S.; WILLIAMS, M. L. - Policing cybercrime: networked and social media technologies and the challenges for policing. **Policing Society**. 23:4 (2013) 409-412. https://doi.org/10.1080/10439463.2013.780222

WALLHOFF, Hanna; TOVE, Hultin - **Combating Money Laundering: AML technologies in money laundering detection, investigation and prevention**. Lund: Lund University, 2020. Available at http://lup.lub.lu.se/student-papers/record/9017634

WESSEL, J. - The financial action task force: A study in balancing sovereignty with equality in global administrative law. **Widener Law Review**. 13 (2006). Available at https://ssrn.com/abstract=895421

YOUNG, Oran R. - **Compliance and Public Authority**. Baltimore: John Hopkins University Press, 1979.

ZAGARIS, B. - **International White Collar Crime. Cases and Materials**. Cambridge: Cambridge University Press, 2010.

ZDANOWICZ, J. - Trade-based money laundering and terrorist financing. **Review of Law and Economics**. 5:2 (2009) 854-878.

ZDANOWICZ, J. S. - Money Laundering AND Terrorist Financing. Communications of the ACM. 47:5 (2004) 53.