MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

„THE ROLE OF EU ELECTRONIC MONEY INSTITUTIONS IN COMBATING MONEY LAUNDERING AND TERRORIST FINANCING“

verfasst von / submitted by

CANAN GİRGİN

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2023 / Vienna 2023

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	UA 992 548
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht / European and International Business Law
Betreut von / Supervisor:	ao. Univ.-Prof. Mag. Dr. Siegfried Fina

ACKNOWLEDGEMENTS

I would like to extend my heartfelt gratitude to my family, whose unwavering support, even from afar, has been an indispensable factor in the completion of this thesis. In particular, I want to express my deepest appreciation to my beloved mother, Zeliha Girgin, for being my constant source of encouragement and inspiration throughout my life.

I am also deeply grateful to my dear spouse and friends who stood by my side and provided invaluable assistance in numerous ways during this journey.

Last but not least, I wish to convey my sincere appreciation and thanks to my supervisor, Dr. Siegfried Fina, for his invaluable guidance and mentorship throughout this study. His expertise and encouragement have been instrumental in shaping the outcome of this research, and I am truly fortunate to have had such a dedicated mentor.

Thank you all from the bottom of my heart for being a crucial part of my journey and for making this accomplishment possible.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AML	Anti-Money Laundering
AMLA	Authority for Anti-Money Laundering and Countering the Financing of Terrorism
AMLD	Anti-Money Laundering Directive (Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, as amended by Directive (EU) 2018/843)
BO	Beneficial Owner
CA	Competent Authorities
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
CRF	*Cellule de Renseignement Financier*, the Luxembourg Financial Intelligence Unit
CSSF	*Commission de Surveillance de Secteur Financier*, the Luxembourg supervisory authority of the financial sector
EBA	European Banking Authority
EDD	Enhanced Due Diligence
EC	European Commission
EU	European Union
EBA	European Banking Authority
ECB	European Central Bank
EMI	Electronic Money Institution
FATF	Financial Action Task Force (international standard-setting body in the field of AML/CFT)
FIU	Financial Intelligence Unit (national enforcement body which receives STRs from OEs and forwards them, as appropriate to criminal investigation authorities)
KYC	Know Your Customer
ML	Money Laundering
OE	Obliged Entity (legal or natural person within the scope of AMLD and subject to AML/CFT rules)

UNODC	United Nations Office on Drugs and Crime
PI	Payment Institution
PSD2	Consolidated Version of the Council Directive 2015/2366 of 25 November 2015 on payment services in the internal market amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TF	Terrorism Financing

ABSTRACT (English)

The rapid digitalization of the financial landscape has given rise to electronic money (e-money) as a digital alternative to traditional cash payments. E-money offers convenience and speed for financial transactions, but it has also opened up opportunities for money launderers and terrorist financiers to exploit. This study explores the role of EU Electronic Money Institutions in combating money laundering and terrorist financing, delving into the conceptual framework of e-money, money laundering and the specific techniques employed in this sector. The study begins with an overview of the regulatory framework of electronic money within the EU, examining past and present e-money regulations and the operations of Electronic Money Institutions under EU directives. It acknowledges the advantages and challenges of e-money, recognizing its facilitative potential and susceptibility to exploitation. Subsequently, the study delves into the concept of money laundering and the illegal activities associated with it, emphasizing its global threat. The definition and stages of money laundering, including its connection to terrorism financing, are explored, with a focus on the intertwining of electronic money with money laundering. The study analyzes money laundering techniques involving e-money and discusses the EU's measures and regulations to combat this issue. The final chapter highlights the crucial steps that EMIs must take to counter money laundering attempts involving electronic money. By implementing preventive measures, EMIs can play a pivotal role in combatting illicit activities and safeguarding the integrity of the EU financial system. This study aims to contribute to the understanding of potential vulnerabilities and effective measures to counter money laundering activities in the digital age within the context of the European Union.

ABSTRACT (Deutsch)

Die rasche Digitalisierung der Finanzlandschaft hat zur Entstehung von elektronischem Geld (E-Geld) als digitale Alternative zu traditionellen Bargeldzahlungen geführt. E-Geld bietet Bequemlichkeit und Schnelligkeit für Finanztransaktionen, birgt aber auch einige Gefahren, vor allem im Hinblick auf Geldwäsche und Terrorfinanzierung. Diese Studie untersucht die Rolle der EU-Unternehmen für elektronisches Geld bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung und geht dabei auf den konzeptionellen Rahmen von E-Geld, Geldwäsche und die spezifischen Techniken ein, die in diesem Sektor angewendet werden. Die Studie beginnt mit einem Überblick über den regulatorischen Rahmen für elektronisches Geld innerhalb der EU und untersucht weiters frühere und aktuelle E-Geld-Vorschriften sowie die Geschäftstätigkeit von Unternehmen für elektronisches Geld unter den EU-Richtlinien. Sie erkennt die Vorzüge und Herausforderungen von E-Geld an und erkennt sowohl das fördernde Potenzial als auch die Anfälligkeit für Ausbeutung. Anschließend widmet sich die Studie dem Konzept der Geldwäsche und den damit verbundenen illegalen Aktivitäten und betont ihre globale Bedrohung. Die Definition und Stufen der Geldwäsche, einschließlich ihrer Verbindung zur Terrorismusfinanzierung, werden untersucht, wobei der Fokus auf der Verflechtung von elektronischem Geld mit Geldwäsche liegt. Die Studie analysiert Geldwäschetechniken, die E-Geld einbeziehen, und erörtert die Maßnahmen und Vorschriften der EU zur Bekämpfung dieses Problems. Im letzten Kapitel werden die entscheidenden Schritte hervorgehoben, die Unternehmen für elektronisches Geld unternehmen müssen, um Geldwäscheversuche mit elektronischem Geld zu bekämpfen. Durch die Umsetzung präventiver Maßnahmen können Unternehmen für elektronisches Geld eine entscheidende Rolle bei der Bekämpfung illegaler Aktivitäten spielen und die Integrität des EU-Finanzsystems schützen. Diese Studie zielt darauf ab, zum Verständnis potenzieller Schwachstellen und wirksamer Maßnahmen zur Bekämpfung von Geldwäscheaktivitäten im digitalen Zeitalter im Kontext der Europäischen Union beizutragen.

1. INTRODUCTION

The advent of digitalization has transformed the financial landscape, with global markets and evolving technologies driving significant changes. In this digital era, e-money has emerged as a digital alternative to traditional cash payments. E-money enables individuals to conduct transactions using funds stored on cards, mobile devices, or online accounts. However, as financial transactions increasingly transition to virtual platforms, money launderers and terrorist financiers have taken advantage of globalization and technology to accelerate their illicit activities.

Electronic money and electronic payment systems have become prevalent, offering convenience and speed for financial transactions. However, the growing use of e-money has raised concerns regarding its potential misuse for money laundering purposes, warranting the need to understand the conceptual framework of money laundering and the specific techniques employed in this context. Therefore, this study aims to explore the relationship between money laundering and electronic money by delving into the conceptual understanding of money laundering, the techniques and methods employed, and the role of electronic money institutions in facilitating or combating illicit activities.

After an introduction, the study commences in the 2nd Chapter with an overview of the concept and the regulatory framework of electronic money within the European Union. An in-depth examination of electronic money regulations from past to present is conducted, along with a focus on the operations of EMIs under the EU directives. The chapter further explores the advantages, challenges, and intricacies associated with the use of e-money, acknowledging both its facilitative potential and susceptibility to exploitation.

The 3rd Chapter of the study delves into money laundering and the illegal activities associated with it, emphasizing the significant threat it poses globally. Furthermore, the concept of money laundering is explored. In the subsequent chapter, the study explores the definition and stages of money laundering, specifically concentrating on the relationship between money laundering and terrorism financing. Additionally, an assessment is made of how electronic money intertwines with money laundering. The chapter analyzes money laundering techniques involving e-money, underscoring the critical importance of comprehending these methods to combat illicit practices effectively. Within this context, the measures and regulations set forth by the European Union to combat money laundering are also discussed.

Finally, the 4th Chapter focuses on the essential steps EMIs must take to counter money laundering attempts involving electronic money. By understanding and implementing necessary preventive measures, EMIs can play a pivotal role in the fight against illicit activities and protect the integrity of the EU financial system.

In conclusion, this study aims to shed light on the intersection of money laundering and electronic money within the European Union context. Through a comprehensive examination of money laundering practices, e-money regulations, and the role of EMIs in combating financial crimes, this study endeavours to contribute to the understanding of potential vulnerabilities and effective measures to counter money laundering activities in the digital age.

1.1. Purpose of the Research

There is general information related to the concept of money laundering from the proceeds of crime, money laundering methods, the stages involved, money laundering and terrorist financing risks in the e-money sector, and the role of EMIs in fighting against money laundering. The purpose of the study is to evaluate the crucial role of EMIs in combating money laundering, the associated risks, and measures or recommendations to prevent those risks.

1.2. Methodology

The study was carried out as a qualitative analysis and complied with the rules and regulations accordingly. As a main method for the research, documentary analysis is used. The information used is obtained from existing legal sources. The study is based on the research of various written texts on the subject and will be utilized as an analysis of any existing literature and legislation. The legal texts used in this thesis include journals, reports, articles, presentation papers, and textbooks. The study is analyzing the upcoming directives and regulations; therefore, in order to get information about them, internet resources will play a crucial role. The publications from the European Commission will be key in determining the current state and development of the laws that are relevant to the topic. Since the laws are under consideration at the time of this thesis writing process, some of the sections of the relevant laws can already be amended.

2. ELECTRONIC MONEY IN THE EUROPEAN UNION

2.1. Notion and Meaning of Electronic Money

Studies on the phenomenon of electronic money, or e-money, which at that time only comprised pre-paid cards, are based on an initial study of the ECB conducted in 1993 and published in its report in 1994.[1] Electronic money is now broadly defined by the ECB as "an electronic store of monetary value on a hardware-based or software-based technical device"[2] but at that time it was only concentrated on card-based products such as multipurpose prepaid card or « electronic purse » meaning electronic cash on chipcards with the possibility to make payments.[3]

The Group of Ten[4] defines electronic money as

"Electronic purses or stored-value cards and prepaid or stored-value payment mechanisms for executing payments over open computer networks, such as the Internet."[5]

As e-money has been subject to EU regulation for the first time in Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, it has an established regulatory framework. The Legal definition of the e-money is stated in Article 1 of this repealed Directive 2000/46/EC[6] as "electronic money shall mean monetary value as represented by a claim on the issuer which is: (i) stored on an electronic device; (ii) issued on receipt of funds of an amount not less in value than the monetary value issued; (iii) accepted as means of payment by undertakings other than the issuer."

Building on the Directive 2000/46/EC, Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC defines e-money as "electronically, including magnetically, stored monetary value as represented by a claim on the issuer that is

---

[1] European Central Bank, *Report on Electronic Money* (European Central Bank August 1988) p. 7

[2] European Central Bank, 'Electronic Money' (*Ecb.europa.eu*) <https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html> accessed on 30 November 2022.

[3] Nathalie Janson, 'The Development of Electronic Money: Toward the privatization of money issue?' (2004) 9(2) Journal of Internet Banking and Commerce p. 11

[4] The Group of Ten is composed of eleven industrial countries (Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom, and the United States) which consult and cooperate on economic, monetary, and financial matters.

[5] Group of Ten, 'Electronic Money: Consumer protection, law enforcement, supervisory and cross border issues' (*Bis.org*, April 1997) Bank for International Settlement <https://www.bis.org/publ/gten01.htm> accessed on 01 December 2022

[6] Council Directive 2000/46/EC of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions [2000] OJ L275/39

issued on receipt of funds for the purpose of making payment transactions …, and which is accepted by a natural or legal person other than the electronic money issuer."[7]

The World Bank adopted a flexible approach in its report with respect to defining e-money in order for it to be differentiated into network money, M-Money, electronic purse, and electronic wallet. Thus, in its 2012 report, it defined e-money as "a record of funds or value available to a consumer stored on a payment device such as chip or magnetic stripe prepaid cards, mobile phones or on computer systems as a non-traditional account with a banking or nonbanking entity."[8]

Considering the rapidly changing and developing nature of digital technology, it is difficult for all organizations and regulators to provide a single and precise definition of electronic money. For this reason, several official bodies are content with making their own definitions of the existing products.

2.2. Electronic Money Regulation in the EU

Electronic money, which emerged as a new type of payment instrument in the 1990s and has since become increasingly prevalent with the rapid advancements in technology and electronic commerce, has been subject to various regulations due to its potential impact on the monetary policies of the EU. With these regulations, the legislator aimed to stimulate developments and competition in the payment sector, encourage new entrants (non-banks) to enter the market and support e-money product innovations in order to establish creating legal certainty.[9]

Electronic money systems, which were first regulated in the EU with the Directive 2000/46/EC, were later amended at several points with the Directive 2005/60/EC, the Directive 2006/48/EC. Later on, European Parliament adopted Directive 2009/110/EC, which introduces new legal regulations specifically pertaining to the issuance and issuers of electronic money. The main objectives of Directive 2015/2366 are also outlined, given the similarities between electronic money services and payment services. Current discussions and legislative packages from the EC that exert the most significant impact on electronic money systems are discussed.

---

[7] Consolidated Version of the Council Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L267/7

[8] The World Bank, I*nnovations in Retail Payments Worldwide: A Snapshot* (The World Bank 2012) p. 3

[9] Malte Krueger, 'E-money regulation in the EU' in Robert Pringle and Matthew Robinson (eds), *E-Money and Payment Systems Review* (Central Banking 2002) p. 239

a) Directive 2000/46/EC

The first e-money directive was published in the Official Journal of the EU on 27 October 2000. This directive provided a clear definition of electronic money and also introduced the concept of electronic money institutions, which were designed as a distinct category of credit institution.[10]

Although the first e-money directive of the European Union is an important driving force for the Member States to draw attention to this new and quickly evolving technology and make detailed arrangements in their domestic laws, it has also been criticized by critics for not being attractive for non-banks to become an EMI and therefore not achieving its main goal due to the following reasons[11]:

- The unclear definition of e-money caused practical uncertainties, as national authorities were left to decide whether to treat a particular body as an e-money institution.[12]
- The restrictive provisions regarding initial capital and ongoing funds requirements, credit lending, ancillary business activities, and permissible investments by e-money institutions limited options for e-money issuers to generate profit through the issuance of e-money.[13]

b) Directive 2005/60/EC[14]

Directive 2005/60/EC was not solely focused on the e-money business, but it requested electronic money institutions to fulfil several rules and requirements as this sector and its products may be linked to money laundering and terrorist financing.[15] In this context, the general rules applied to credit institutions in order to prevent money laundering are also applicable to electronic money institutions. For instance, electronic money institutions were obliged by Directive 2005/60/EC to carry out customer due diligence to identify the customer and verify their identity.

In some cases, e-money institutions may have been exempt from applying CDD if that it is not possible to recharge, the maximum amount stored in the device is no more than EUR 150, or where it is possible to recharge, a limit of EUR 2 500 is imposed on the total amount

[10] ibid.
[11] ibid.
[12] Phoebus Athanassiou, Natalia Mas-Guix, 'Electronic Money Institutions Current Trends, Regulatory Issues and Future Prospects' (July 2008) 7 European Central Bank Legal Working Paper Series p. 12
[13] ibid.
[14] Council Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing [2005] OJ L309/15
[15] Daniel Wilusz, 'Legal determinants of electronic money systems development in European Union' (2011) 2 Pedrawny i ekonomiczny przegląd prawa gospodarczego Wydawnictwo Naukowe UAM p. 125

transacted in a calendar year, except when an amount of EUR 1 000 or more is redeemed in that same calendar year.[16]

This threshold set forth therein has changed from time to time in line with the risk-based approach to electronic money products of the European Parliament and the Council of the EU. On 20 May 2015, the European Parliament and the Council of the EU adopted Directive 2015/849[17], which provided an exception to customer due diligence measures with regard to electronic money if the maximum electronically stored amount does not exceed EUR 250. However, this approach changed after variety of terrorist attacks took place in Europe in 2016. The EC proposed a new set of rules tightening the EU's legal regime on preventing money laundering and terrorist financing and resulting in the adoption of Directive 2018/843[18] amending Directive 2015/849 in 2018. In the amended rules, the threshold amounts, with regard to non-reloadable pre-paid electronic money instruments to which such customer due diligence measures apply, were reduced once again to EUR 150 for non-reloadable pre-paid electronic money instruments. Finally, the threshold for derogation from customer due diligence for remote payment transactions has also been reduced from EUR 100 to EUR 50. By doing so, transparency regarding e-money products was increased, and the anonymity of the e-money products was limited. Thus, the risk of electronic money systems being used for money laundering is clearly lower when transactions are limited to small value payments. While these regulations within the framework of the EU directives significantly reduce the risk of money laundering, they may also pose challenges, such as hindering the development of the e-money sector.

Money laundering and terrorist financing pose significant threats to the integrity of the European economy, financial system, and the safety of EU citizens. As part of their ongoing efforts to reform and standardize the EU's AML/CFT framework, the EC has introduced a set of legislative proposals[19] (hereinafter referred to as the "AML Package") on 20 July 2021. The

[16] Dir 2005/60/EC (n 14) Art 11.5.(d)

[17] Consolidated Version of the Council Directive 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L141/73

[18] Council Directive 2018/843 of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43

[19] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing' (2021) COM 420 final; 'Proposal for a Directive of the European Parliament and of the Council on the mechanisms for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849' (2021) COM 423 final; 'Proposal for a Regulation of the European Parliament and of the Council establishing the European Authority for Countering Money Laundering and Financing of

primary objectives of these proposals are to enhance the EU's AML/CFT regulations, promote transparency, and align the rules with international standards.

It is evident that the EMIs will also be affected by this new set of regulations as one of the obliged entities. For instance, regarding simplified customer due diligence measures mentioned above have simply been deleted without any revision or replacement. Instead, it has been referred to regulatory technical standards which to specify simplified customer due diligence standards for prepaid cards and other e-money products to be developed by AMLA and submitted to the EC for adoption.[20] Further, the proposal suggests that EMIs appoint a central contact point, who will represent the appointing EMI and ensure its compliance with the AML/CFT rules, in consideration of the anti-money laundering vulnerabilities that have been witnessed in the electronic money sector specifically.[21]

Finally, the ECB published its opinion on this package of legislative proposals on 16 February 2022 and mostly welcomed the initiative and supported the strengthening of the AML/CTF regime in the EU.[22] The opinions provided by the ECB are likely to significantly influence the ongoing legislative process, and the final version of the regulations affecting the e-money sector and EMIs is yet to be determined.

c) Directive 2006/48/EC[23]

Directive 2006/48/EC, published in the Official Journal of the EU on 30 June 2006, aimed to facilitate the establishment and operation of credit institutions. Pursuant to Article 4/1(b) of this directive, electronic money institutions were initially classified as credit institutions. However, this provision was later repealed by Directive 2009/110/EC, which bestowed a sui generis identity upon electronic money institutions.

d) Directive 2009/110/EC

Terrorism, amending Regulations (EU) No 1093/2010 (EU) 1094/2010 and (EU) 1095/2010' (2021) COM 421 final; and 'Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets' (2021) COM 422 final

20 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing' (2021) COM 420 final Art. 22

21 European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the mechanisms for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849' (2021) COM 423 final Art 5.1

22 European Central Bank, 'Opinion of the European Central Bank of 16 February 2022 on a proposal for a regulation establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism' (2022) C 210/05

23 Council Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions (recast), OJ L 177, 30.06.2006, p. 1.

The ambiguity surrounding Directive 2000/46/EC was apt to lead to adverse outcomes contrary to the spirit of Directive 2000/46/EC. Ongoing discussions at that time emphasized the importance of categorizing EMIs based on clear and unequivocal criteria, as continuing to treat them as credit institutions could lead to adverse outcomes contrary to the spirit of Directive 2000/46/EC.[24] Hence, it was essential to amend the definition of e-money, reconsider the concept of an e-money institution, and review the waiver regime. These measures were deemed necessary to foster continuous growth in the electronic money sector and unlock the full potential benefits that were initially anticipated.[25] Similarly, the proposal of the European Commission for a new electronic money directive specifically highlighted that certain provisions of Directive 2000/46/EC appeared to hinder the take-up of the electronic money market and hamper technological innovation.[26] The primary goal of the proposal for the new electronic money directive was "*to enable new, innovative and secure electronic money services to be designed, provide market access to new players and foster real and effective competition between all market participants*".[27]

The European Parliament took a significant step in updating the electronic money directive, Directive 2009/110/EC, which now includes several new and harmonized legal rules and regulations concerning electronic money. The revisions in the directive offer an improved legislative framework, serving as a solid foundation for the development of electronic money services.[28] This change allows EMIs to operate without being classified as traditional credit institutions, offering more flexibility and opportunities for non-bank entities to provide electronic money services. Additionally, the directive broadens the list of entities permitted to issue electronic money, potentially leading to a more diverse and competitive market for electronic money issuance. Overall, these changes are expected to foster innovation and growth in the electronic money sector, benefiting consumers and businesses alike.

Further, the definition of electronic money has been clarified in order to make it technically neutral and has broadened its scope to cover not only current electronic money products but also those products to be developed in the future. Furthermore, according to Article 4 of the Directive 2009/110/EC initial capital requirements were reduced from EUR 1,000,000

[24] Athanassiou, Mas-Guix (n 12)
[25] ibid.
[26] European Commission, 'Proposal for a Directive of the European Parliament and of the Council of on the taking up, pursuit and prudential supervision of the business of electronic money institutions, amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC' (2008) COM/2008/0627 final
[27] ibid.
[28] Ruth Halpin, Roksana Moore, 'Developments in electronic money regulation – the Electronic Money Directive: A better deal for e-money issuers?' (2009) 25 Computer Law & Security Review p. 567

to EUR 350,000. Rules and conditions on the application for waivers from authorities were simplified by requiring only that the total outstanding electronic money that does not exceed EUR 5,000,000 and, that none of the natural persons responsible for the management or operation of the business has been convicted of offences relating to money laundering or terrorist financing or other financial crimes.[29]

Furthermore, Directive 2009/110/EC amended the Customer Due Diligence (CDD) thresholds specified in Directive 2005/60/EC by raising the maximum amount stored in non-rechargeable devices from EUR 150 to EUR 250. Ultimately, modernised, and harmonised rules introduced with the Directive 2009/110/EC provided the increased interest in electronic money licenses and cross-border activity by removing barriers to market entry.[30] As anticipated by the EC, the new Directive 2009/110/EC provided e-money market with a second chance to take off, with volumes anticipated to reach up to EUR 10 billion by 2012.[31] With the help of removal of regulatory barriers to issuing e-money and investments in technologies and infrastructure paid off and changed the total amount of e-money transactions dramatically over the years. Numbers of the use of e-money as a payment instrument increased year by year. In 2021, the number of e-money transactions in the EU amounted to around EUR 7,4 billion.[32]

e) Directive 2015/2366[33]

PSD2 was published in the Official Journal of the EU on 25 November 2015 mainly aiming at further integration and supporting a more efficient single EU payments market, as well as promoting competition in an environment where new players such as FinTech start-ups and a new generation of payment products and services are emerging.[34] The main focus of PSD2 is to establish rules regarding the transparency of conditions and information requirements for payment services, as well as the rights and obligations of payment service

---

[29] Dir 2009/110/EC (n 7) Art 9.1
[30] European Commission, 'Report from the Commission to the European Parliament and the Council on the implementation and impact of Directive 2009/110/EC in particular on the application of prudential requirements for electronic money institutions' (2018) COM/2018/041 final
[31] European Commission, 'European Commission welcomes the European Parliament's adoption of two proposals in the area of payments (on e-money and cross-border payments)' (*Ec.europa.eu*, April 2009) <https://ec.europa.eu/commission/presscorner/detail/en/IP_09_637> accessed on 26 December 2022
[32] Reynor de Best, 'Number of e-money purchase transactions in the European Union from 2000 to 2021' (*Statista.com*, March 2023) <https://www.statista.com/statistics/443399/electronic-money-payment-in-european-union/> accessed on 24 March 2023
[33] Consolidated Version of the Council Directive 2015/2366 of 25 November 2015 on payment services in the internal market amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35
[34] Markos Zachariadis, Pınar Özcan, 'The API Economy and Digital Transformation in Financial Services: The Case of Open Banking' (June 2017) 2016-001 Swift Institute Working Paper 2016-001, p.4 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975199> accessed on 24 March 2023

users and providers.[35] As a result, in conjunction with Directive 2009/110/EC, PSD2 sets minimum standards for conduct and security that all participants in the electronic payments market, including existing and new players, must comply with.[36]

In order to make EU payments market safer and more secure, PSD2 introduces enhanced security measures, in particular the requirement to apply two-factor strong customer authentication (SCA), to be implemented by payment service providers, including electronic money institutions. In pursuit of this objective, the EBA provides support for the implementation of PSD2 and develops Regulatory Technical Standards to ensure the fulfillment of PSD2's objectives. Since EMIs are one of the payment service providers mentioned in PSD2, they are also affected by the rules and ongoing discussions concerning its implementation. Recent discussions and opinions from the EBA indicate that PSD2's objectives have begun to materialize. However, several significant issues need to be addressed to achieve these objectives more comprehensively.[37] In the opinion dated 23 June 2022, EBA set forth its findings on the implementation of PSD2, a number of proposals and recommended that the EC revises the PSD2 to address these issues and areas for improvement of the legal requirements.

The EBA has put forth a notable proposal concerning the amalgamation of PSD2 and Directive 2009/110/EC. According to the EBA, this merger presents an excellent opportunity to standardize the legal framework's application, making it more efficient and straightforward for PIs and EMIs to comply with the requirements. he primary goal is to prevent regulatory arbitrage and ensure fairness in the treatment of various payment service providers, promoting technological and business model neutrality and creating a future-proof legal foundation.[38] Depending on how the merger is executed, it could bring about changes in the regulation of EMIs and e-money issuance, potentially leading to a more effective and unified approach.

2.3. Issuers of Electronic Money

2.3.1. Electronic Money Issuer v. Electronic Money Institutions

Directive 2009/110/EC sets out two different definitions, i.e. the "electronic money issuer" and the "electronic money institution". Directive 2009/110/EC recognizes electronic money issuers, and they are listed in Article 1(1) as follows:

---

[35] Dir 2015/2366 (n 33) Art 1

[36] Stefan Loesch, *A Guide to Financial Regulation for Fintech Entrepreneurs* (John Wiley & Sons, Incorporated 2018) p.184

[37] European Banking Authority, 'Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)' (23 June 2022) EBA/Op/2022/06

[38] ibid.

a) credit institutions as defined by Directive 2006/48/EC;
b) electronic money institutions;
c) post office giro institutions which are entitled to issue electronic money under national law;
d) the European Central Bank and national central banks when not acting in their capacity as monetary authority or other public authorities;
e) Member States or their regional or local authorities when acting in their capacity as public authorities.

As evident from the Article, EMIs represent one category among the aforementioned issuers of electronic money. Directive 2009/110/EC defines an electronic money institution as "a legal person that has been granted authorization under Title II to issue electronic money".[39] For an electronic money institution to issue electronic money, it must fulfill several specific requirements, such as meeting the initial capital requirement[40], maintaining its own funds[41], conducting appropriate activities[42] and safeguarding the funds[43]. These requirements are specific to the electronic money institutions and do not apply to other electronic money issuers.

For the purposes of this research, the requirements for the taking up of the business of electronic money institutions, which are among the electronic money issuers, in order to fulfil their activities will be discussed in detail.

2.3.2. Main Requirements to Electronic Money Institutions

In order to issue electronic money, electronic money institutions, which are specifically regulated under the Directive 2009/110/EC, must fulfil the requirements stated in Directive 2009/110/EC, as well as the relevant provisions of Directive 2015/2366, which apply *mutatis mutandis*. These requirements, which are designed to ensure an appropriate level of consumer protection and to operate electronic money institutions soundly and prudently, are as follows:

- To be authorized as an EMI, the institution shall submit an application to the competent authorities of its home Member State and subsequently be registered within the European Union.

[39] Dir 2009/110/EC (n 7) Art 2.1
[40] Dir 2009/110/EC (n 7) Art 4
[41] Dir 2009/110/EC (n 7) Art 5
[42] Dir 2009/110/EC (n 7) Art 6
[43] Dir 2009/110/EC (n 7) Art 7

- Electronic money institutions shall possess, at the time of authorization, an initial capital of not less than EUR 350.000.[44]
- Electronic money institutions shall hold, at all times, own funds calculated pursuant to one of the three methods as stated therein in line with the activities of the electronic money institution. Nevertheless, the own funds requirement of an electronic money institution for the activity of issuing electronic money shall be calculated with the Method D and therefore shall amount to at least 2% of the average outstanding electronic money.[45]
- In addition to issuing electronic money, electronic money institutions are permitted to engage in various activities, including the provision of payment services, operational services, and closely related ancillary services, as well as operating payment systems. However, it is important to note that, unlike credit institutions, electronic money institutions are not authorized to accept deposits or other repayable funds from the public.[46]
- Electronic money institutions shall have a registered office in home Member State and have effective head office where it carries out at least part of their principal activity in the same Member State.[47]
- Electronic money institutions shall provide guarantees of sound and prudent management of the electronic money institution itself, further shall have robust governance arrangements in place for its business activities, including a clear organizational structure with well-defined, transparent, and consistent lines of responsibility throughout, efficient process for identifying, managing, monitoring and reporting the risks to which it is or might be exposed, and adequate internal control mechanisms, including sound administrative and accounting procedures.[48]
- Electronic money institutions shall have the adequate internal control mechanisms with respect to fulfil with its obligations in relation to money laundering and terrorist financing.[49]

[44] Dir 2009/110/EC (n 7) Art 4
[45] Dir 2009/110/EC (n 7) Art 5.3
[46] Dir 2009/110/EC (n 7) Art 6
[47] Dir 2015/2366 (n 33) Art 11.3
[48] Dir 2015/2366 (n 33) Art 11.4
[49] Dir 2015/2366 (n 33) Art 5

However, some electronic money institutions, particularly the smaller ones, may qualify for an exemption from these authorization requirements and operate under a waiver if they can demonstrate the following conditions:

a) Their total business activities generate an average outstanding electronic money that does not exceed a limit set by the Member State but that, in any event, amounts to no more than EUR 5 000 000; and
b) None of the individuals responsible for the management or operation of the business have been convicted of offences relating to money laundering or terrorist financing or other financial crimes.[50]

2.4. The Use of Electronic Money

Technological advancements have significantly impacted the economy and payment systems, giving rise to new payment instruments. In the realm of e-commerce, cash usage has been limited, and even traditional brick-and-mortar shops are increasingly embracing cashless payment options. Major retail companies are now experimenting with electronic payments in their stores.[51] Research conducted by the ECB has highlighted the key factors that customers value in payment methods: broad acceptance, ease of use, low cost, high speed, security, and consumer protection. Merchants, on the other hand, prioritize low cost, ease of use, and integration with existing systems.[52] Current studies indicate that 55% of consumers in the euro area consumers prefer using cards or other cashless means of payment due to the various benefits it offers. The convenience of cashless payments is a primary driver, as people no longer need to carry physical cash.[53] Given the widespread usage of electronic devices today, e-money has the potential to gain broader acceptance if it can competitively meet economic, functional, and consumer protection criteria compared to other payment instruments. This could pave the way for electronic money to replace cash in various transactions.

However, it's essential to recognize that electronic money, like other payment instruments, presents both advantages and disadvantages. This study will explore the benefits

---

[50] Dir 2009/110/EC (n 7) Art 9.1

[51] Jorg Snoeck, 'Ikea trials cashless store in the Netherlands' (*Retaildetail.eu*, 3 September 2019) <https://www.retaildetail.eu/news/home/ikea-trials-cashless-store-netherlands/> accessed on 10 February 2023.

[52] Christine Lagarde, Fabio Panetta, 'Key objectives of the digital euro' (*The ECB Blog,* July 2022) <https://www.ecb.europa.eu/press/blog/date/2022/html/ecb.blog220713~34e21c3240.en.html> accessed on 10 February 2023.

[53] Ulrich Bindseil, Doris Schneeberger, 'Cash or cashless? How people pay' (*The ECB Blog*, 6 February 2023) <https://www.ecb.europa.eu/press/blog/date/2023/html/ecb.blog230206~1ea270a762.en.html> accessed on 10 February 2023.

and obstacles associated with using electronic money in comparison to cash and other payment methods under separate headings.

2.4.1. Benefits of the use of Electronic Money

Electronic money, issued in accordance with EU regulations, serves an efficient means of payment and fosters innovation in the digital age. Its benefits include cost reduction, decreased check and credit card fraud, lower risk of theft and vandalism in retail outlets, and enhanced convenience for consumers, all of which further contribute to its widespread adaptation. By using e-money, individuals gain access to a diverse range of payment opportunities while eliminating the need for face-to-face transactions. This enables users to make purchases promptly and in larger amounts, promoting more seamless payment experiences. Some electronic money applications even allow multiple currencies to be stored on a single smart card, enabling users to make payments in various currencies without the burden of carrying cash. As a result, a single payment instrument simplifies cross-border transactions, ensuring ease and security for users. Additionally, the elimination of a physical wallet, spares users the challenges of handling cash such as weight and hygiene concerns, making the payment process more efficient and time-saving.

Smart cards, widely used for e- money, have proven highly effective in preventing fraud and money laundering. Each money transaction made with e-money is meticulously recorded, and the electronic value and other stored information on the smart card are safeguarded by a robust algorithmic password structure. This renders counterfeiting electronic money or the smart card itself a costly and formidable task, making electronic money a secure option for users.

In addition to the advantages it offers to electronic money users, it also benefits merchants who accept electronic money payments. The streamlined process of electronic money transactions facilitates the collection of payments, minimizing the risk of late payments and related issues. Furthermore, the fixed cost per transaction for electronic money payments is significantly lower compared to traditional payment methods, providing merchants with cost-saving benefits.

2.4.2. Obstacles of the use of Electronic Money

Although electronic money offers various benefits, it also presents certain obstacles and risks as a payment instrument, with security being a primary concern. While counterfeiting electronic money is a challenging and costly endeavor, unauthorized access to computer networks can lead to the draining of e-money accounts or disruptions in the operation of the electronic money system due to viruses or similar programs.

Additionally, power or line interruptions may render the electronic value inaccessible for use, causing delays in payment transactions. Maintaining the security and uninterrupted operation of the electronic money system is crucial to ensure a seamless user experience and prevent potential financial losses.

Another significant concern is the issue of anonymity, as privacy protection must be upheld in accordance with applicable laws. Like any payment method, e-money systems can potentially be exploited for illicit purposes, such as money laundering, confidentiality breaches, and tax evasion. Striking a balance between comprehensive record-keeping for the prevention of money laundering and respecting the privacy rights of users becomes essential to address these issues effectively.

Preserving the privacy of private data and information in electronic money payment transactions is pivotal for the advancement of electronic money systems. Addressing these challenges will not only enhance the security and reliability of electronic money but also contribute to building trust among users, enabling the sustainable growth of this payment method.

3. CONCEPTUAL FRAMEWORK OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE EU AND ROLE OF E-MONEY SECTOR IN MONEY LAUNDERING

In this chapter, the concepts of dirty money, money laundering, terrorism, and terrorist financing, which constitute the illegal activities within the informal economy, have been clarified. Additionally, in order to comprehensively understand the conceptual framework of ML/FT and the role of the e-money sector in money laundering, the various stages of money laundering and how electronic payment systems, including electronic money institutions, are exploited as a means to launder illicit proceeds, have been thoroughly examined.

3.1. Definitions of Dirty Money and Money Laundering

In its broadest sense, dirty money is defined as any proceeds that are illegally earned, transferred, or utilized. Dirty money can be categorized into three different forms: criminal, corrupt, and commercial.[54] To identify dirty money and its form, it is essential to examine the source of the proceeds of crime. When analyzing black money according to its source, it can be evaluated under two sub-headings. In the first group, criminal and corrupt, the profit obtained from the very beginning of the incident is acquired through an offence. For example, money derived from drug trafficking, slave trading, bribery and theft by public officers, and financing of terrorism belongs to the first group. In the second group, while everything starts on a legal basis, the money is obtained by causing public damage as a result of tax evasion in the form of false invoices or forgery of documents forgery.

When defining dirty money, a single definition should be avoided, considering that dirty money activities have effects in multiple societal areas. Examining the effects of dirty money in detail reveals its primary economic impact, as well as some social, legal, and moral deterioration in society. Therefore, dirty money should be defined differently in economic, social, moral, and legal terms. Economically, it refers to any gain obtained by violating the rules governing a country's economic activities. Socially, dirty money encompasses all proceeds deemed inappropriate by society, causing harm to society, social life, and social welfare, even indirectly. Morally, black money includes any proceeds obtained in violation of social moral rules and the general perspective of society, regardless of whether they are recognized as a crime in the country's legislation. Legally, black money encompasses all benefits obtained by converting money, negotiable instruments, goods, income, and currencies from transactions and actions determined as predicate offenses in the legislation of the country.

Proceeds of crime defined in Vienna Convention, refer to any property derived from or obtained, directly or indirectly, through the commission of an offence.[55] Considering that technology and the opportunities it provides can be misused by criminals in new and various ways, therefore the term "property" herein refers to assets of every kind, whether corporeal or incorporeal, movable, or immovable, tangible or intangible, and legal documents or instruments evidencing title to or interest in such assets.

Without prejudice to differences in legal definitions across jurisdictions, criminal codes and regulators, money laundering is an international crime, broadly defined as the concealment and seeking legitimization of the criminal or illicit source of the proceeds of a crime.[56] This

---

[54] Thomas W. Dunfee, Colleen Baker, 'Review: The Impact of Dirty Money on Global Capitalism' (2007) 17(4) Business Ethics Quarterly p. 729

[55] United Nations, 'United Nations Convention against Transnational Organized Crime and the Protocols Thereto' (2004) p. 5

[56] U.S. Congress, Office of Technology Assessment, '*Information Technologies for the Control of Money Laundering*' (U.S. Government Printing Office, September 1995) p. 35

legitimization process, known as the laundering process, involves routing illicit money through a chain of multiple transactions, disguising its origin, nature, source, location, ownership, and disposition, giving the impression of having come from a legitimate source. In parallel, FATF, an international standard setter for combating money laundering and financing of terrorism, characterizes money laundering as the act of concealing the illicit origins of the proceeds from criminal activities.[57]

3.2. Definitions of Terrorism and Terrorist Financing

Given that there is not one and clear definition of terrorism, as widely acknowledged by the majority of academics, terrorism can be described as intentional acts of injuring, endangering, or killing security forces or civilians by individuals belonging to an organization, usually for political purposes, with the intention of creating disruption and dissatisfaction within the country. Although financial gain is not the primary objective for these terrorist entities and individuals, they do require economic resources to sustain their activities to carry out their terrorist acts – this is referred to as terrorist financing.

The funding sources of terrorist organizations vary from dues and donations to social events, legal commercial enterprises, etc. These funds can be acquired through both legal and illegal means. For example, terrorists employ a wide range of methods to move money within and between organizations, including the financial sector, the use of couriers for physical money transfers, and the movement of goods through the trading system.[58] Furthermore, charities and alternative remittance systems have been exploited as means to conceal the movement of terrorist funds. While the funds themselves might be obtained through legal channels, their use for financing activities that renders them illegal. As such, any person providing or collecting funds for an individual or organization engaged in terrorist activities, regardless of whether the sources of financing are legal or illegal, is considered to have committed the crime of terrorist financing.

In 2001, the FATF included combating terrorist financing in its anti-money laundering strategies and defined terrorist financing as the financial support of terrorist acts, terrorists and terrorist organizations.[59]

---

[57] FATF, 'What is Money Laundering?' (*Fatf-gafi.org*) <https://www.fatf-gafi.org/en/pages/frequently-asked-questions.html#tabs-36503a8663-item-6ff811783c-tab> accessed on 20 March 2023.

[58] Central Bank of Bahrain, 'Combating the Financing of Terrorism Guidance for Financial Institutions' (*Cbb.gov.bh*, November 2020) <https://www.cbb.gov.bh/wp-content/uploads/2021/10/Guidance-Paper-Combating-the-Financing-of-Terrorism_17-Nov-2020.pdf> accessed on 20 March 2023.

[59] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF Recommendations' (updated February 2023) <https://www.fatf-

3.3. Stages of Money Laundering

In order for the proceeds of crime to be integrated into daily life and to introduced into the economic system as if obtained legally, they must be undergo a process of laundering that involves multiple transactions, evading the scrutiny of state institutions. The advancement of technology leads to the emergence of new and diverse methods for legitimizing these proceeds on a daily basis. Despite the variety of methods, laundering activities generally consist of three basic stages: placement, layering and integration.[60] At each of these stages, illicit funds gain a legal identity and become explainable. The analogy of washing dirty laundry can help illustrate these stages: First, the dirty money needs to be somehow incorporated into the financial system, akin to pre-washing. The second step, washing, involves erasing the link between the asset value and its original source, completely removing any trace of its illicit origins. The third and final stage is the drying stage, during which the "cleaned" money is invested in legitimate assets. The goal is to ensure that the money is "dried" of any suspicion, making it appear as though it hasn't undergone numerous financial transactions.

While these three stages are generally used in money laundering activities, each stage may involve multiple transactions. In other words, even within each stage, the asset value may be divided, and the stages may be completed in various ways. Studies show that the more techniques used, the more effectively cash can be laundered or concealed.[61] For instance, during the placement stage, the asset value arising from the crime can be introduced into the economic system by dividing it into parts, without the need for a single significant transaction. In practice, it is not mandatory to follow these stages precisely and in order, as each laundering operation may vary according to its own unique circumstances. Additionally, AML laws worldwide do not distinguish crimes based on placement, layering or integration, making such terminology more of a jargon rather than a recognition of the ingenuity or fluidity of laundering schemes.[62] For this reason, it is appropriate to explain each stage in detail separately.

3.3.1. Placement

gafi.org/content/dam/recommandations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf> accessed on 23 March 2023

60 Timothy H. Ehrlich, 'To Regulate or Not - Managing the Risks of E-Money and Its Potential Application in Money Laundering Schemes' (1998) 11 Harv J L & Tech 833 p. 835

61 Angela Samantha, Maitland Irwin, Kim-Kwang Raymond Choo, 'An analysis of money laundering and terrorism financing typologies' (December 2011) 15(1) Journal of Money Laundering Control p. 105

62 FATF, 'Professional Money Laundering' (26 July 2018) < https://www.fatf-gafi.org/en/publications/Methodsandtrends/Professional-money-laundering.html> p.22

The fact that proceeds of crime mostly exist in physical form poses challenges using them for payments through the financial system or transferring them to other individuals or financial institutions. Hence, the first stage of laundering is the "placement" stage, where the illicit proceeds are converted into other forms to integrate them into the legal financial system.[63] The presence and use of significant amounts of cash can draw attention, so it is essential to convert the proceeds into alternative forms, such as real estate, jewelry, cryptocurrencies, artwork, luxury cars, gold, and other valuables. Similarly, the funds can be physically transported to countries with limited controls, divided into smaller amounts, and deposited into various ATMs and banks within the current country. According to the EC Report dated 27 October 2022, sectors/products like cash couriers, cash payments, the private banking sector, fund transfers, crypto-assets, high-value assets (precious metals and stones), investment real estate, gambling, etc., are commonly used in the placement stage.[64]

The primary objectives of the placement phase are twofold: to free the offender from holding large sums of illegally obtained cash and to integrate the illicit money into the legitimate financial system.[65] Consequently, this stage is considered the most challenging and risky for money launderers, while it offers advantages to authorities and obligated entities due to the strong link between the assets and the crime.[66] Establishing a strong connection between the crime and the illicit proceeds is crucial for understanding and proving the origin of the assets. Therefore, the measures taken during this stage and the reporting and detection of suspicious transactions are of paramount importance.

3.3.2. Layering

During the layering stage, the proceeds of crime undergo a series of complex financial transactions that mimic legitimate activities. These transactions vary in frequency, volume, and complexity, with the ultimate aim of severing the link between the value of the illicit funds and their criminal source, thereby concealing the origin of the proceeds.[67] Compared to the placement stage, this phase is relatively easier for money launderers but poses significant

---

[63] UNODC, 'Money Laundering' (*Unodc.org*, April 2018) <https://www.unodc.org/e4j/en/organized-crime/module-4/key-issues/money-laundering.html> accessed on 1 April 2023.
[64] European Commission, 'Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market relating to cross-border activities' (2022) COM/2022/554 final
[65] UNODC (n 63)
[66] Samantha, Irwin, Choo (n 61)
[67] Financial Crime Academy, 'The Three Stages of Money Laundering: The Characteristics of the Money Laundering Stages' (*Financialcrimeacademy.org*) <https://financialcrimeacademy.org/the-three-stages-of-money-laundering/> accessed on 2 April 2023.

challenges for investigative and supervisory mechanisms. In the layering stage, launderers employ electronic transfers to move the illicit proceeds across borders through offshore bank accounts, effectively camouflaging their source. One method exploited by launderers involves abusing the correspondent banking relationship, wherein two banks from different countries establish a correspondent account allowing a local bank to conduct transactions on behalf of a foreign bank in local currency. Shell companies are also frequently utilized in the layering process, enabling the concealment of true account holders at offshore correspondent financial institutions. The usage of large sums of money, numerous transactions, various fraud schemes, and a domestic bank's unfamiliarity with the customers of foreign correspondent banks allows criminals to easily obscure the source and utilization of unlawful funds. For example, Al Qaeda utilized the correspondent network of a Sudanese bank for cross-border dealings involving France's Credit Lyonnais and Germany's Commerzbank.[68]

Considering the advancements in technology and the surge of electronic transfers, it is essential to recognize that laundered proceeds can be challenging to trace during this stage. The duration of the layering phase depends on the launderer's assessment of how effectively the proceeds are concealed from detection and their confidence that competent authorities will not trace them.

3.3.3. Integration

After completing the placement and layering stages, the final phase of money laundering, integration, is initiated to introduce the crime proceeds, now disconnected from their illicit origins, into the legitimate economic financial system. Unlike the earlier stages that focused on disguising the illicit funds, the integration phase serves the purpose of using the laundered money for various legitimate purposes. The funds, which initially existed in cash form and underwent various complex financial transactions during layering, are now seamlessly integrated into the financial system and ready for lawful use.[69]

At this stage, satisfactory explanations can be provided to judicial authorities and financial institutions regarding the source of the money. Consequently, the integration stage represents the weakest link to the original crime, making it more challenging to establish a direct connection between the proceeds and the criminal activity compared to the previous

[68] Silvia Allegrezza, 'The proposed Anti-Money Laundering Authority, FIU cooperation, powers and exchanges of information: A Critical Assessment' (July 2022) Publication for the committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.

[69] UNODC (n 63)

stages. As a result, identifying the link between the illicit proceeds and the crime becomes particularly difficult during the integration phase.

3.4. Money Laundering Through with Electronic Money

Money laundering and terrorism financing involve transactions aimed at disguising illegally earned proceeds as legitimate by using various methods. These activities pose a significant threat to the economic, political, and social structures of countries and continue to evolve with advancements in informatics, technology, and new payment methods. In addition to traditional laundering methods (such as smurfing, shell companies, stock exchanges, exchange offices, casinos, etc.) conducted through financial institutions, money launderers are exploring new avenues using non-financial institutions and professional agencies to exploit the internet and e-money products for their illicit purposes. As e-money becomes an integral part of emerging technology and payment systems, it, too, falls victim to manipulation by cyberlaunderers.[70]

This section aims to understand how cyber-laundering is executed through e-money and to present a comprehensive analysis of the risks and vulnerabilities related to money laundering and terrorist financing in the e-money sector.

Before delving into the risk scenario and the contributing factors that exposing the e-money sector to ML/TF risks, it is essential to emphasize the main characteristic of electronic money – its pre-paid nature. This means that the value of e-money is loaded onto an online account, card, or mobile device.[71] While many e-money products require identification and customer due diligence, certain exemptions permit owners to remain anonymous. This feature of e-money creates a risk scenario for ML/TF, as perpetrators can either use anonymous e-money products directly (without any customer identification) or indirectly by abusing non-anonymous e-money products (through deception, using straw men, stolen, or fake identities.).[72] Though abusing non-anonymous e-money products is not always cost-effective, launderers may prefer this option due to its relative ease in dealing with intermediaries in the delivery channel. Nevertheless, e-money products may still be a preferred choice over cash for

---

[70] Jonathan P. Straub, 'The Prevention of E-Money Laundering: Tracking the Elusive Audit Trail' (2002) 25 Suffolk Transnat'l L Rev 515 p. 533

[71] European Commission Report (n 64)

[72] ibid.

ML/TF purposes, especially when serving as a substitute for bulk cash transportation or taking advantage of non-face-to-face service provisions to use straw men or stolen identities.[73]

Possible example of the emergence the ML/TF risk as follows:

a) Perpetrators can load multiple anonymous prepaid cards, optionally abroad with limited traceability, using recourses and values stemming from illicit sources. Then can transfer funds from the prepaid card account to bank accounts for cash pay-outs or further money transfers.
b) Perpetrators can load multiple anonymous prepaid cards, optionally abroad with limited traceability, using recourses and values stemming from illicit sources. These prepaid cards can then be used to make various purchases of goods, which are later sold to other parties.

According to the EBA Opinion on ML/TF risks, the main contributing factors that expose e-money sector to ML/TF risks include the common use of intermediaries within distribution channels, making adequate oversight challenging.[74] Additionally, the sector's reliance on non-face-to-face identification processes, use of false documents, an increase in computer fraud, and the ease and speed of e-money transactions are indicated as key risks.[75] The EBA Opinion also highlights that the lack of a limit on the number of prepaid cards a customer may own also contributes to ML/TF risks in the e-money sector.

A recent EBA report also highlights a growing trend known as white labelling within the e-money sector. This practice involves EMIs granting their licenses to independent agents who offer their own financial products under the licensed institution's umbrella. This practice has led to a diverse range of financial products available in the market. It has been highlighted the challenges faced by EMIs in effectively integrating these white-labelled products into their AML/CFT frameworks and noted that it can be difficult for EMIs to comprehensively assess and address the corresponding risks associated with these products, as well as monitor and control the risks arising from such activities.[76]

E-money becomes an attractive method of money laundering when it can be purchased with cash and used online and offline, especially when loaded onto prepaid cards or vouchers

[73] Hanafi Amrani, 'The Development of Anti-money Laundering Regime: Challenging Issues to Sovereignty, Jurisdiction, Law Enforcement, and Their Implications on the Effectiveness in Countering Money Laundering' (Doctoral thesis, Erasmus University Rotterdam 2012) p.35
[74] European Banking Authority, 'Opinion on Money Laundering and Terrorist Financing Risks Affecting The EU Financial Sector' (3 March 2021) EBA/Op/2021/04 para. 96
[75] EBA Opinion on ML/TF risks (n 74) para. 97
[76] European Banking Authority, 'Opinion on Money Laundering and Terrorist Financing Risks Affecting The EU's Financial Sector' (13 July 2023) EBA/Op/2023/08 para. 162

benefiting from CDD exemptions, representing a large sum of money. Additionally, prepaid cards sold by distributors who are not obliged entities without full customer due diligence also increase the level of money laundering threat related to e-money.[77] When we assess the terrorist financing threat linked to e-money products, the risk scenarios mentioned in money laundering applies *mutatis mutandis*. There is evidence that e-money loaded onto prepaid cards has been used in hotel payments and car rentals and therefore has been an attractive way for helping terrorist acts.[78] Given the rapid and easy movement of large transactions using e-money products and the possibility of easy physically transporting prepaid cards to high-risk jurisdictions for terrorism, tracking perpetrators and criminal organizations can become challenging even sufficient transaction monitoring.[79]

Due to the wide range of products in the e-money sector, it is difficult to determine its complete vulnerability. As mentioned above, some cash-based e-money products not linked to a current account and are exempt from customer due diligence measures are more vulnerable than other bank account or payment account-based e-money products, resembling anonymous cash.[80] Additionally, the suitability of e-money for a single phase of ML or a combination of various payment systems can enhance its favorability for the ML process.[81] Consequently, while launderers operate in a traceable environment on the internet, e-money offers them an appealing opportunity to conceal the origin of money and remain anonymous[82], contributing to the vulnerability of the e-money sector to money laundering and terrorist financing.

3.5. Current Regulatory Scheme Established to Combat Money Laundering and Terrorist Financing in the EU

3.5.1. Introduction

Since its establishment, the European Union has pursued various objectives, including enhancing economic, social, and territorial cohesion and solidarity among its Member States, establishing an economic and monetary union, and promoting scientific and technological progress.[83] In pursuit of these goals, the EU has put in place a comprehensive framework of

[77] European Commission Report (n 64)
[78] ibid.
[79] ibid.
[80] ibid.
[81] Krzysztof Woda, 'Money Laundering Techniques With Electronic Payment Systems' (2006) 18 Information & Security Journal p. 45
[82] Brigitte Unger & Johan den Hertog, 'Water always finds its way: Identifying new forms of money laundering' (2012) 57 Crime L & Soc Change 287 p. 298
[83] European Union, 'Aims and Values' (*European-union.europa.eu*) <https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-

AML/CFT directives and regulations, aligning with international standards of FAFT recommendations. These regulations apply to all Member States and financial institutions operating within the EU, with the primary aim of combating money laundering and terrorist financing. This regulatory regime plays a crucial role in contributing to international security, ensuring the integrity of the financial system, safeguarding citizens' security, and fostering sustainable growth. To ensure the effectiveness of the AML/CFT regulatory framework, the EU has also established several institutions and bodies responsible for overseeing its implementation and enforcement. These include the European Banking Authority (EBA), the European Central Bank (ECB), Europol, and Financial Intelligence Units (FIUs) in each Member State.

3.5.2. EU AML Legislation

In the EU, the fight against money laundering and terrorist financing, which is considered one of the most complex financial crimes, is conducted by adopting international regulations related to this matter and incorporating them into the national laws of the Member States. The EU also updates its regulations over time to align with the latest international documents and address the evolving threats posed by technological advancements and the intricate tools employed in the financial world. Consequently, EU regulations significantly mirror the developments in this field at the international level and remain in parallel with the FATF Recommendations.[84]

In the subsequent sections of this study, through an examination of the European Union directives, the formation of the AML/CFT regime across the EU and how it has changed and developed over time will be emphasized, taking into account the historical order.

a) First AML Directive[85] (Council Directive 91/308/EEC of 10 June 1991)

On June 10, 1991, the 1st AML Directive was adopted by the Council of Ministers in order to fight against money laundering. The aim of the Directive 91/308 was to prevent the use of the financial system as a means money laundering while ensuring the free flow of capital and the access to financial services.

---

values_en#:~:text=achieve%20sustainable%20development%20based%20on,the%20quality%20of%20the%20environment> accessed on 1 May 2023.

[84] Valsamis Mitsilegas, Bill Gilmore, 'The EU Legislative Framework Against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards' (January 2007) 56 International and Comparative Law Quarterly p. 120

[85] Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering [1991] OJ L166

The First AML Directive was founded on the principles of the Vienna Convention and the recommendations of the FATF. It held a significant role in broadening the scope of criminal activities subject to scrutiny, encompassing proceeds from various crimes, not just drug offenses.[86] Additionally, it imposed obligations on credit and financial institutions concerning customer identification, record-keeping, and reporting of suspicious transactions.[87]

However, the First AML Directive did not specify the entity to which these suspicious activities should be reported by credit and financial institutions for aggregation and analysis.[88] This lack of clarity resulted in Member States having discretion in designating these entities, leading to the establishment of various models of national authorities. For instance, such authorities could be an interdependent unit within a government department, a police officer and/or intelligence agency or even a judicial authority.[89] While international information flow and cooperation between FIUs of the Member States and other national authorities is necessary for better anti-money laundering efforts, this have been problematic as the various national authorities established by Member States had often had difficulties in communicating and cooperating among each other. To address these challenges, EU Member States adopted EU Council Decision 2000/642/JHA[90] to facilitate cooperation between FIUs, enabling the exchange of information on potential money laundering cases, regardless of the legal status of the FIU.

b) The Second AML Directive[91] (Council Directive 2001/97/EC of 4 December 2001)

The Second AML Directive was developed in response to the evolving nature of money laundering and the necessity to address emerging risks as money launderers continually seek and develop alternative methods for laundering through technology and concealing the origin of the proceeds of crime.

In 1996, the FATF 40 Recommendations underwent a revision, resulting in a redefined laundering offense. While the previous regulations covered only drug trafficking as the predicate offense, the scope was expanded with the revision. Subsequently, Directive

[86] Norman Mugarura, 'Customer Due Diligence (CDD) Mandate and the Propensity of its Application as a Global AML Paradigm' (2014) 17(1) Journal of Money Laundering Control p. 77
[87] Konstantinos D. Magliveras, 'The European Community's Combat Against Money Laundering: Analysis and Evaluation' (1998) 5 ILSA Journal of International & Comparative Law p. 97
[88] Cian C Murphy, *EU Counter-Terrorism Law : pre-emption and the rule of law* (Hart Publishing 2015) p. 95
[89] Mitsilegas, Gilmore (no 84) p. 122
[90] Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information [2000] OJ L271
[91] Council Directive 2001/97/EC of 4 December 2001amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering [2001] OJ L344

2001/97/EC was issued in order to incorporate these changes from international regulations into EU legislation and to enhance the fight against laundering according to higher standards.

While the EC emphasized that the primary objective of the Second AML Directive was to strengthen the preventive pillar established by the First AML Directive and combat new money laundering methods, it also extended the scope of predicate offenses and professional groups obliged to implement prevention measures.[92] The Second Directive broadened the range of obliged entities and activities covered by EU AML regulations, mandating financial institutions, including banks, credit institutions, insurance companies, and other entities engaged in financial activities, to implement robust AML measures. As a pivotal point, the Second AML Directive laid the foundation for subsequent EU AML directives, which further fortified the AML framework and expanded its scope to address emerging risks, technological advancements, and the global AML/CFT standards set by the FATF.

c) The Third AML Directive 2005/60/EC[93]

The Third AML Directive adopted on 26 June 2005, aimed to strengthen the AML/CFT framework of the EU, building upon the foundation laid by the previous AML directives and taking into account international standards, particularly those set by the FATF. This directive was introduced to effectively address emerging challenges and risks related to money laundering and terrorist financing. Its primary objectives were to bolster the EU's AML framework, harmonize regulations across Member States, and enhance cooperation and information sharing among relevant authorities.

Before the introduction of the Third AML Directive, there were several pressing challenges in the field of money laundering and terrorist financing that demanded attention. These included difficulties in tracking and monitoring the movement of funds due to globalization and cross-border transactions, as well as challenges in identification and traceability posed by cybercrime, virtual currencies and online payment systems.

Furthermore, in response to the terrorist attacks in the USA on September 11, 2001, the FATF issued nine specific recommendations on measures to combat the financing of terrorism. To ensure these measures were consistently adopted by the Member States[94], the Third AML Directive was implemented, aiming to tackle the emerging challenges and risks by introducing

---

[92] Emmanuel Ioannides, *Fundamental Principles of EU Law Against Money Laundering* (Ashgate Publishing Company 2014) p. 48

[93] Dir 2005/60/EC (n 14)

[94] Jayesh D'Souza, *Terrorist Financing, Money Laundering And Tax Evasion: Examining The Performance Of Financial Intelligence Units* (CRC Press, 2011) p. 105

enhanced measures for due diligence, beneficial ownership transparency, risk assessment, and cooperation among Member States.

d) The Fourth AML Directive 2015/849/EC[95]

On May 20, 2015, the EU adopted the Fourth AML Directive which implemented a newer and stricter EU AML/CTF legal regime within the EU. While building on the framework established by the Although the Fourth AML Directive built on the framework established by the Third AML Directive (which it repealed), the Fourth AML Directive introduced significant structural changes, improved consistency, and strengthened previous directives aimed at combating money laundering and terrorist financing.[96] The Fourth AML Directive places strong emphasis on risk assessment and adopts a corresponding risk-based approach. It also broadens the scope of obliged entities, strengthens rules for identifying beneficial owners of companies and trusts, and mandates the maintenance of a national register of beneficial owners in all EU Member States. Additionally, it introduces harmonized European policies to address deficiencies in anti-money laundering and counter-terrorist financing policies of non-EU Member States, underscores the need to enhance international cooperation between financial intelligence agencies. As a result, the Fourth AML Directive marks a significant milestone in the EU's ongoing efforts to combat money laundering and terrorist financing. By addressing key vulnerabilities, promoting transparency and prioritizing aforementioned objectives, it aims to strengthen the EU's AML/CFT framework.

Prior to this, in 2012, the FATF, the most influential and significant organization in the fight against money laundering and terrorist financing, updated its recommendations. As previously mentioned, the FATF recommendations play a crucial role as a catalyst for the European Union's efforts against money laundering, serving as a model for legislators to enact and for Member States to implement in their legal systems.[97]

e) The Fifth AML Directive 2018/843/EC[98]

Particularly, serious concerns were raised related to the new financial tools and payment modes after the heinous terrorist attacks in the EU in 2015. These concerns highlighted the

[95] Dir 2015/849/EC (n 17)
[96] Pierpaolo Fratangelo, *The New Anti-Money Laundering Law: First Perspectives on the 4th European Union Directive* (Palgrave Macmillan, 2016) p. 11-12
[97] Patricia Godinho Silva, 'Recent developments in EU legislation on anti-money laundering and terrorist financing' (2019) 10(1) New Journal of European Criminal Law p. 60
[98] Dir 2018/843/EC (n 18)

need for a strong, coordinated response and additional rules to fight against ML/TF.[99] In response to this pressing need, the proposal to amend the Fourth AML Directive and introduce the Fifth AML Directive was put forward in 2016 and subsequently adopted by the European Parliament in 2018.

The Fifth AML Directive takes into account the increasing popularity of certain modern technology services that act as alternative financial systems, operating outside the scope of EU law or benefiting from various legal exemptions. The directive and aims to ensure increased transparency of transactions conducted out through these services. To achieve this, the scope of the Fifth AML Directive is extended to include exchange services providers (dealing between virtual currencies and fiat currencies) and custodian wallet providers, which were not previously subject to EU obligations to report suspicious transactions.[100] Additionally, the directive also brings persons involved in storing, trading or acting as intermediaries in the trade of works of art, including art galleries and auction houses, within the scope of reporting obligations, preventing money laundering through the use of works of art as investment instruments.[101]

Another novelty introduced by the Fifth AML Directive is the empowerment of the EC to identify third countries that pose a high risk for money laundering and terrorist financing.[102] EDD measures will be applied to business relationships or transactions involving high-risk third countries.[103] Moreover, to ensure timely access to information by national FIUs and/or other competent authorities, the Fifth AML Directive prescribes all Member States to establish a central registry containing information on the identity of holders of the bank and payment accounts, as well as their proxy holders and their beneficial owners.[104] However, it should be noted that while the structure of the new regulations is one aspect; the effective application of these regulations through transposition by the Member States is another matter. Recognizing that AML/CFT rules are instrumental in the fight against money laundering and terrorist financing, the EC urges Member States to comply with their obligations under EU law. In a recent package of infringement decisions, the EC calls on Italy, Latvia, and Portugal to correctly transpose the Fifth AML Directive into national law, emphasizing the need to

[99] European Commission, 'Commission presents Action Plan to strengthen the fight against terrorist financing' (E*c.europa.eu*, 2 February 2016) <https://ec.europa.eu/commission/presscorner/detail/en/IP_16_202> accessed on 2 May 2023.
[100] Dir 2018/843/EC (n 18) Preamble
[101] Dir 2018/843/EC (n 18) Art 1/1
[102] Dir 2018/843/EC (n 18) Art 1/5
[103] Dir 2018/843/EC (n 18) Art 1/11
[104] Dir 2018/843/EC (n 18) Preamble

address non-conformities such as the obligation to register, license or regulate service providers (Italy and Latvia), the obligation to establish a payment and bank accounts register (Latvia) and ensuring proper access to anti money laundering information for the FIU (Portugal).[105]

Therefore, it is crucial to be reminded that the fight against ML/TF is a cross-cutting issue that requires joint action, involving the cooperation and convenient functioning of FIUs, ministries, supervisors, and law enforcement authorities at the national level, as well as their cooperation at the EU level.

f) The Sixth AML Directive[106]

Despite substantial enhancements to the AML/CFT regulatory framework over the years at the national and EU levels, challenges related to technological innovation, such as crypto assets, remain. Following several cases of alleged anti money laundering involving EU credit institutions, the EC analyzed the cases and revealed that credit institutions had substantially failed to comply with main AML legislative requirements, including risk assessment, CDD, and reporting of suspicious activities and transactions to FIUs. Consequently, the EC concluded that EU AML/CFT regulatory framework requires updates in order to keep pace with new developments.[107]

In 2020, the EC presented a new Action Plan to establish a stronger and more comprehensive EU policy on preventing money laundering and countering the financing of terrorism. The Action Plan identified a lack of detail in applicable rules, resulting in divergent interpretations of the AML/CFT regulations. It also highlighted inadequate cooperation among competent authorities, including national FIUs, supervisors, law enforcement, customs and tax authorities, leading to potential loopholes.[108] To address these issues, the EC committed to implementing a comprehensive AML/CFT policy tailored to specific risks, threats and vulnerabilities that the different sectors are currently facing. This Action Plan is building on six pillars as follows:

1. Ensuring the effective implementation of the existing EU AML/CFT framework.

[105] European Commission, 'European Commissions – Infringement decisions' (*Ec.europa.eu*, April 2023) <https://ec.europa.eu/commission/presscorner/detail/en/inf_23_1808> accessed on 2 May 2023.
[106] Proposal for a Directive (n 21)
[107] European Commission, 'Communication from the Commission to the European Parliament and the Council towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework' (2019) COM 360 final
[108] European Commission, 'Communication from the Commission to the European Parliament and the Council on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing' (2020) C 164/21

2. Establishing an EU single rule book on AML/CFT.
3. Establishing EU level AML/CFT supervision.
4. Establishing a support and cooperation mechanism for FIUs.
5. Enforcing EU-level criminal law provisions and information exchange.
6. Strengthening the international dimension of the EU AML/CFT framework.[109]

To implement this Action Plan, as previously explained, the EC presented a comprehensive package of legislative proposals including the new Sixth AML Directive, AML/CFT Regulation, a regulation providing for the creation of AMLA and a revision of the Regulation 2015/847 on Transfers of Funds to trace transfers of crypto-assets. On 19 April 2023, the EU Parliament announced the approval of its negotiating mandate for the proposed AML Package.[110] Details of recent risk-mitigating measures regulated and new measures proposed by AML Package to be taken by EMIs will be introduced in following section. Understanding the key features of the new AML Package is important.

One of the key elements of this AML Package is the creation of AMLA, a new supervisory authority aimed at establishing consistent and effective supervision throughout the EU Member States. AMLA will provide a common, consistent methodology for assessing and identifying risks and to applying a risk-based approach.[111] In addition to the direct supervision of some of the obliged entities, AMLA shall coordinate national FIUs, assist them reinforcing their quality and effectiveness in enforcing rules and shall play an important role in developing the information exchange and cooperation between national FIUs.

To address the difficulties in the field of AML/CFT outlined above, the forthcoming AML Package also contains a single EU rulebook on AML/CFT, specifying rules such as the list of the obliged entities, CDD requirements, CDD threshold for occasional transactions, and beneficial ownership transparency to be applied by obliged entities throughout the EU internal market. The single rulebook will introduce more harmonized and directly applicable rules, eliminating current fragmentation with regard to AML/CFT obligations for the obliged entities and the activities of competent authorities.[112]

---

[109] Action Plan (n 108)

[110] European Parliament, 'Stopping the flow of dirty money: Parliament ready for negotiations' (Europarl.europa.eu, 19 April 2023) <https://www.europarl.europa.eu/news/en/press-room/20230414IPR80123/stopping-the-flow-of-dirty-money-parliament-ready-for-negotiations> accessed on 16 May 2023.

[111] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council establishing the European Authority for Countering Money Laundering and Financing of Terrorism, amending Regulations (EU) No 1093/2010 (EU) 1094/2010 and (EU) 1095/2010' (2021) COM 421 final

[112] Proposal for a Regulation (n 20) Preamble

To implement all pillars defined above, another legislative action is required. The proposed the Sixth AML Directive repeals and replaces the existing Fifth AML Directive, as amended by Forth AML Directive. The EC emphasized that the Sixth AML Directive, building on previous AML directives, is also consistent with the FATF recommendations and consolidates the latest revisions.[113] The Sixth AML Directive will contain substantial changes concerning cooperation among national FIUs, including clarification of powers and tasks, rules on feedbacks from FIUs to obliged entities, and the introduction of a common risk-categorization tool. The proposed changes and provisions are intended to improve the consistency of the AML/CFT framework's implementation across the EU.[114] Another part of the AML Package is the regulation on information accompanying transfers of funds and certain crypto-assets aiming to strengthen the AML/CFT rules and policies of EU, to trace the origin and/or destination of transfers of crypto assets. The Council of the EU emphasized that the regulation will ensure financial transparency on exchanges of crypto-assets and enhance the traceability of virtual asset transfers.[115]

4. MEASURES AGAINST MONEY LAUNDERING AND EMI'S ROLE

The anti-money laundering system has two pillars: preventive measures to prevent money launderers from using private individuals and institutions for their illicit activities, and criminal law enforcement that intercedes when money laundering offenses occur despite these preventive measures.[116] The preventive measures regulated in this context include certain obligations and responsibilities imposed on obliged entities to ensure that transactions are recorded, thereby deterring money laundering and the utilization of high-risk sectors for this purpose. Additionally, these measures mobilize law enforcement to initiate criminal prosecution and to access evidence. The main elements of the prevention pillar encompass: (i) customer due diligence to prevent launderers from gaining access to the financial system or other money laundering mechanisms, (ii) notifications that draw the attention of relevant authorities to transactions that are likely related to ML/TF, (iii) supervision of obliged entities' compliance with anti-money laundering legislation, and (iv) sanctions against individuals and

---

[113] Proposal for a Directive (n 21) Preamble

[114] Thomas Wahl, 'AML Package III: 6th AML Directive Proposed' (*Eucrim.eu*, 5 August 2021) <https://eucrim.eu/news/aml-package-iii-6th-aml-directive-proposed/> accessed on 16 May 2023

[115] European Council, 'Anti-money laundering: Council adopts rules which will make crypto-asset transfers traceable' (*Consilium.europa.eu*, 16 May 2023) <https://www.consilium.europa.eu/en/press/press-releases/2023/05/16/anti-money-laundering-council-adopts-rules-which-will-make-crypto-asset-transfers-traceable/> accessed on 19 May 2023.

[116] Peter Reuter, Edwin M. Truman, *Chasing Dirty Money: The fight Against Money Laundering* (Peterson Institute for International Economics, 2004) p. 46

institutions failing to implement the prevention regime and breaching their obligations and duties in this regard.[117] Through these preventive measures, the illicit actions and launderers are being closely monitored. On the other hand, the criminal law pillar, being of a secondary nature, consists of the list of predicate offenses that serve as the legal basis for regulating money laundering as a type of crime, the investigation and prosecution process to identify concrete instances of money laundering, and confiscation.

Preventive measures aim to combat crime before it is committed, thereby safeguarding public order and reducing the occurrence of ML/TF actions, and ultimately minimizing the social and economic costs associated with combating such of combating such crimes. Conversely, criminal law measures act as a last resort, coming into effect after the crime has occurred and targeting the criminals themselves. Therefore, criminal law enforcement considered secondary to preventive measures, as the prevention pillar focuses on individuals and institutions at high risk of becoming money laundering intermediaries.[118]

As mentioned above, what is foreseen from the prevention pillar of the anti-money laundering regime is to make it more difficult to commit ML/TF crimes, to identify launderers who were previously unknown to the authorities and to initiate investigations against them, to support investigations into known or suspected money launderers and to uncover evidence, to prevent the transfer of money out of the EU, and to discourage launderers from committing crimes by making them think that they cannot subject the proceeds to any transaction.[119]

The main basis for these preventive measures lies in legal regulations and international studies. As extensively explained in detail in the previous sections, the need to combat ML/TF crimes has been addressed at the international level under the guidance of FATF recommendations, followed by the establishment of ML/TF regime through EU legal regulations, and the transposition of these regulations into the domestic laws of EU Member States. Given the vital role of EMIs and e-money systems in the EU financial systems, the diversion of illicit or even legal money for terrorist purposes poses a clear risk to the integrity, proper functioning, reputation, stability, and development of the e-money sector. Consequently, EMIs, among other obliged entities, bear significant responsibility to identify, assess, and comprehend the ML/TF risks they may encounter. Based on these risks, EMIs need

[117] ibid.
[118] Reuter, Truman (n 116) p. 47
[119] Michael Levi, *Money Laundering: Risks and Countermeasures* (Australian Institute of Criminology, 1996) p. 1

to ensure the full and complete implementation of specific preventive measures proportionate to the identified risks.[120]

In this section of the study, I will begin by examining the diverse range of measures that EMIs are required to implement in order to prevent ML/TF activities. Following that, I will present an overview of financial intelligence units, which are national institutions established in accordance with the AML legislation of EU Member States. Finally, I will provide an overview of Luxembourg's own financial intelligence unit, known as The Cellule de Renseignement Financier.

4.1. Types of Preventive Measures

4.1.1. Know Your Customer and Customer Due Diligence

One of the most fundamental aspects of the fight against money laundering in the e-money sector is the due diligence obligation of licensed EMIs which comprises the identification and verification of all customers and all individuals acting on their behalf. The duty of CDD is stemming from the need to ensure that EMIs comply with the obligations set out in laws and regulations, including the need to establish sufficient systems and controls to mitigate the risk of EMIs being involved in money laundering and terrorist financing activities. The level and depth of the CDD measure shall be fulfilled by EMI in accordance with the principle of the risk-based approach and in line with EMI's risk appetite, not only by obtaining and recording customer information and documents but also by establishing a risk management system that shall assess the products and service channels used by customers against the risk of ML, ranking them from high to low probability of exposure to risk.[121] It is clear that the CDD is one of the effective security measures adopted in the fight against ML, based on the idea that it would be beneficial for financial institutions to know their customers and take necessary measures to be implemented that are commensurate to the ML/TF risks to be identified. In order to prevent the transfer of proceeds of crime into the financial system through e-money, EMIs are required to identify the customer by collecting certain customer details of the person making the transaction, to verify those details in an effort to confirm the customer is who they say they are, and to keep the identity information for possible cases. The content of the identity information mentioned here is the basic identity or registration information that distinguishes the person from other persons, so in fact, "identification" is a phrase that summarizes the

---

[120] Pietro Pavone, Francesco Parisi, 'Compliance and Corporate Anti-Money Laundering Regulation' (2018) 7(2) Journal of Governance and Regulation p. 9

[121] Dennis Cox, *Handbook of Anti Money Laundering* (John Wiley & Sons, 2014) p.169

identification of the customer well in terms of content. For natural persons, information such as name, surname, passport number, nationality, residential address, and date and place of birth are the basic information for customer identification, while for legal entities, information such as full legal name, tax identification number, business address, nature of business and source of funds constitute the basic information for customer identification. To mitigate the associated risks resulting from dealing with high-risk customers, EDD may also include additional steps to validate information provided by the customer, and/or the utilization of the internet or other means to conduct additional research about the customer.

The obligation to establish CDD identification is regulated in international legal instruments as the first stage of preventive measures. Indeed, Recommendation 10 of the FATF Recommendations[122] in the preventive measures section requires the financial institutions to undertake CDD measures in certain cases and to verify the identity of the customers and beneficial owners using reliable, independent sources.

As mentioned above, EMIs shall determine the degree and framework of safeguards in this case based on a risk-based approach. Each new customer and existing customer should undergo the same assessment, as the duty of care continues even after the establishment of the relationship between the EMI and the customer. FATF Recommendation 12[123] states that additional measures to the CDD should be taken in respect of foreign politically exposed persons and their family members and relatives. Thus, measures will be taken against the risk of these persons taking advantage of their position to gain unfair advantage.

In line with the FATF Recommendations, current EU legal laws and regulations have also imposed CDD obligations upon OEs, and further, the AML Regulation proposed as part of the AML Package has further clarified the existing provisions on CDD and introduced more specific and detailed provisions on customer identification and verification, simplified and EDD measures are specified in detail. In order to identify natural and legal persons, AMLA, a supervisory authority, is authorized and required to create regulatory technical standards. These standards will contain a list of documents to be required for identification of natural and legal persons and will also contain specific rules on simplified CDD measures.[124]

Following the identification of the customer, it is necessary to ensure that the information and supporting documents are kept up to date and that there are no inconsistencies between the transactions to be carried out and the customer's profile and transaction history. This is because

[122] FATF Recommendations (n 59)
[123] ibid.
[124] Proposal for a Regulation (n 20) Preamble

outdated information on EMIs' clients will weaken risk management. It should not be forgotten that the AML/CFT policies and procedures established under the know-your-customer principle are also critical to the integrity, security, and soundness of the e-money sector. In this respect, inadequate or non-existent know-your-customer standards may cause EMIs to lose credibility and confront serious problems such as operational, reputational, and legal risks.[125]

4.1.2. Transaction Monitoring, Suspicious Activity Reporting and Record Maintenance

Transaction monitoring, reporting, and record maintenance play crucial roles in AML/CFT while being part of a broader framework aimed at ensuring the integrity of the financial system and preventing illicit activities. EMIs are required to implement robust transaction monitoring systems to detect and identify transactions that exhibit unusual patterns or characteristics associated with ML and/or TF. These systems analyse customer transactional data in real-time and flag those that exhibit unusual patterns, large amounts, frequent transfers, or involve high-risk jurisdictions. Early detection of suspicious activities enables EMIs to take appropriate action and report such activities to the relevant authorities. Further, by monitoring customer transactions, EMIs can assess the level of risk associated with different customers, products, services, and jurisdictions. This risk assessment enables EMIs to implement appropriate risk mitigation measures, such as EDD procedures, transaction restrictions, or closer scrutiny of high-risk transactions. Effective transaction monitoring also helps EMIs identify and address potential vulnerabilities within their operations. By identifying and addressing potential vulnerabilities, EMIs can ensure compliance with EU AML/CFT regulations. This not only protects the integrity of their operations but also helps maintain trust and confidence among their customers and stakeholders. Additionally, effective transaction monitoring allows EMIs to stay ahead of emerging risks and adapt their risk management strategies, accordingly, enhancing their overall risk management framework.

EMIs are subject to EU AML regulations, including reporting obligations outlined in the EU AML directives. The importance of reporting for EMIs is reinforced in Articles 33 and 34 of the Fifth AML Directive. While Article 33 requires OEs, including EMIs, to report suspicious transactions to the related FIUs, Article 34 provides guidelines on the content and format of SARs, ensuring consistent and effective reporting. The sixth AML Directive, once implemented, will introduce additional and clearer reporting obligations and measures to

[125] Venkatesh U. Rajput, ‘Research on Know Your Customer (KYC)’ (2013) 3 International Journal of Scientific and Research Publications p. 1

enhance the reporting framework. Another reform envisaged to be implemented with the AML Package is to ensure that these suspicious transactions are reported to the relevant FIUs easily and in the same manner across the EU through the technical standards that are binding templates to be issued by the AMLA. This will not only facilitate obliged institutions in fulfilling their reporting obligations but will also enable FIUs to work more effectively and cooperatively.

In order to help EMIs fulfil their legal obligations and reduce the risk of non-compliance penalties, reporting suspicious transactions in accordance with the EU AML regulations demonstrates a commitment to upholding the highest standards of AML/CFT compliance. When suspicious activities are detected, EMIs can file Suspicious Activity Reports (SARs) with the Financial Intelligence Unit (FIU) or other designated authorities. The relevant FIUs evaluate SARs received from OEs and prepare analyses and statistical data based on these reports. Consequently, there is an opportunity to use this data to identify the latest ML trends, methods, sectors, and channels. Timely and accurate reporting of suspicious transactions is essential to support law enforcement efforts, investigate illicit activities, and prevent money laundering and terrorist financing. Reporting suspicious transactions contributes to the sharing of information and intelligence among regulatory authorities, law enforcement agencies, and other OEs. Moreover, it is worth mentioning that compliance with these regulations is crucial for EMIs to maintain their licenses and reputations. The information reported by EMIs can be analyzed and connected with data from other sources to uncover broader networks involved in ML and TF. This collaborative approach strengthens the effectiveness of AML/CFT efforts, enhances knowledge about evolving typologies, and supports the development of more targeted and effective preventive measures.

Overall, transaction monitoring is essential for EMIs to fulfil their AML/CTF obligations, detect suspicious activities, mitigate risks, and contribute to the broader efforts to combat ML/TF. It helps maintain the integrity of the financial system, protects EMIs from being exploited for illicit purposes, and supports regulatory compliance. Non-compliance and failure to report SARs by EMIs can result in steep penalties, reputational damage, and legal consequences for EMIs.

Effective record-keeping plays a crucial role in conducting investigations and uncovering illicit activities, making it an essential component of preventative measures. OEs are required to share all information, documents, and records fully and accurately upon request from FIUs and to keep them ready for audit. This not only helps in identifying potential risks and suspicious transactions but also ensures transparency and accountability within the EMIs.

By maintaining comprehensive records, OE can effectively collaborate with law enforcement agencies and regulatory bodies to combat ML and maintain the integrity of the EU financial system.

4.1.3. Compliance Programs and Compliance Officer

The compliance programs implemented by EMIs play a crucial role in their AML/CFT efforts. These programs are designed to ensure compliance with the set of rules and standards set by the FAFT and the EU. Directive (EU) 2015/849 highlights the significance of this compliance function by mandating that credit or financial institutions, including Electronic Money Institutions, appoint AML/CFT compliance officers at the management level. These programs facilitate the establishment of policies and procedures, risk assessment and reporting processes, and training programs to ensure compliance with these standards. They enable EMIs to detect, assess, and mitigate AML/CFT risks effectively.

Effective compliance programs include the creation and implementation of AML/CFT policies and procedures tailored to the specific risks faced by EMIs. Risk assessment and management are integral parts of AML compliance programs and serve as the foundation for developing effective compliance policies. These policies cover customer due diligence, transaction monitoring, reporting obligations, and other relevant areas. Integrating risk assessment into compliance policies enables EMIs to ensure that their compliance efforts are targeted, proportionate, and effective in mitigating ML/TF risks. Regularly updating risk assessments and adapting policies accordingly allows EMIs to stay proactive in managing emerging risks and regulatory changes.

Compliance officers play a critical role in the effective implementation of AML/CFT policies. Their responsibilities extend beyond simply reporting suspicious activities to financial intelligence units. Compliance officers act as the bridge between regulatory requirements and the OEs, ensuring their full and active participation in the AML/CFT process. Within the framework of compliance programs, they provide guidance, training, and education to employees within the EMI, ensuring a clear understanding of the regulatory framework and compliance expectations. These training programs help employees understand the risks associated with ML/TF. It raises their awareness of suspicious activities and enables them to recognize red flags or indicators that may suggest potential illicit transactions. Besides, trainings foster a culture of compliance within the organization. When employees are educated about AML regulations and their roles and responsibilities in reporting suspicious activities, they are more likely to adhere to compliance policies and actively contribute to the prevention of ML. By having a vigilant workforce, the EMIs can minimize the risk of unknowingly being involved in ML activities and avoid potential regulatory penalties or reputational damage.[126]

Furthermore, ongoing monitoring and review of the effectiveness of these policies are essential to identify any potential gaps or areas for improvement in the AML/CFT framework. By implementing these programs under the supervision of the compliance department, EMIs can enhance their ability to identify and prevent money laundering and terrorist financing activities. This not only helps protect the integrity of the financial system but also safeguards the reputation and trust of the EMI among its customers and stakeholders.

4.2. Financial Intelligence Units

4.2.1. General Information

Financial intelligence units are the institutions mandated by EU member states under the EU's anti-money laundering legislation to assess and, if necessary, forward the reports made by OEs to the competent authorities. The primary objective of the FIU is to gather and evaluate received information from OEs, aiming to establish connections between suspicious transactions and the underlying criminal behavior. This is done to prevent and counteract ML/TF.[127] Additionally as stated, the FIU shares the outcomes of its analysis, along with any supplementary information, with the relevant authorities when there are reasonable suspicions of ML, related underlying crimes, or the TF. These units are central institutions that combine information from various sources to identify individual pieces of evidence that OEs may not be able to detect, thereby uncovering signs of ML/TF that may require further investigation.[128] The vast amount of financial information resulting from reporting and record-keeping obligations is not beneficial to law enforcement authorities without undergoing specific examinations. FIUs possess the expertise to conduct detailed analyses, examining gains suspected of being derived from crime and potential sources of financing terrorism, in accordance with legislation and regulations addressing the fight against ML/TF.

Given that ML and TF are not only threats and problems within EU Member States but also international in nature, the sharing of financial information at both the national and international levels and strong communication between the FIUs of different Member States are essential. In this regard, an unofficial group was established by a group of FIUs in Brussels at the Egmont Palace in 1995 to benefit from the advantages of creating an information-sharing

[126] Pavone, Parisi (n 120) p. 13
[127] Dir 2015/849/EC (n 17) Preamble
[128] Cox (n 121) p. 31

network among these units.[129] Subsequently, this informal group, named the Egmont Group after the location of its first meeting, regularly convened for the purpose of cooperation, training, and sharing expertise, primarily focusing on information exchange. The definition and objectives of FIUs within the Egmont Group align precisely with FATF Recommendation 29 and EU ML/TF rules and regulations. Similarly, each Member State is required to establish a FIU to prevent, detect, and effectively combat ML/TF according to Article 32 of the Fourth AML Directive.

Although the organizational structure and functioning of FIUs may vary from country to country, they are generally expected to perform three fundamental functions: receiving, analyzing, and disseminating suspicious transaction reports and other information related to potential money laundering and terrorist financing activities.[130] Additionally, they may assume secondary responsibilities such as conducting research in their respective fields, providing recommendations to the government and related institutions, and providing feedback to OEs.[131]

The first function of FIUs, "information collection," entails receiving suspicious transaction reports and other reports required by national legislation. Considering the number of OEs, including EMIs, and the likelihood of numerous reports due to their cautious approach, FIUs are at the center of intensive information flow. The value of this data lies in the analysis conducted by the unit.

The "analysis" function of FIUs involves systematically gathering information that could serve as evidence in a potential investigation of ML/TF. This includes assembling meaningful sets of information, formulating assumptions about the activities of suspects based on this information, and identifying new trends, methods and suspicious activities in ML/TF while identifying weaknesses in the country's national legislation.[132]

Financial intelligence units perform the "dissemination" function at both national, EU, and international levels. Firstly, when there is a perception that ML/TF crimes have been committed based on the analysis of information, the relevant file is forwarded to law enforcement agencies or prosecutors, depending on the country's domestic law. Secondly, the obtained findings are shared with other authorized entities outside the police and prosecutors' domains to assist them

---

[129] 'Egmont Group of Financial Intelligence Units' (*Wikipedia*) <https://en.wikipedia.org/wiki/Egmont_Group_of_Financial_Intelligence_Units> accessed on 2 July 2023.

[130] Paul Allan Schott, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (2. World Bank Publications, 2006) p. VII-4

[131] Waleed Alhosani, *Anti-Money Laundering: A Comparative and Critical Analysis of the UK and UAE's Financial Intelligence Units* (Palgrave Macmillan UK, 2016) p. 93-94

[132] Alhosani (n 131) p. 90-91

in fulfilling their functions.[133] This includes information that indicates administrative rule violations or can be used to generate statistics. Lastly, information exchange is conducted with foreign FIUs in a mutually beneficial manner.[134] By converting and disseminating this information into meaningful intelligence, the FIU enables law enforcement agencies and relevant authorities to initiate investigations, prosecute criminals, and effectively disrupt illicit financial networks. In essence, the FIU's central role as an information converter and intelligence provider is paramount in the global effort to combat ML/TF.[135]

4.2.2. The Cellule de Renseignement Financier

In the context of combating ML/TF, Luxembourg has established a robust legal framework and dedicated enforcement units responsible for enforcing these laws and prosecuting offenders. This section focuses on the efforts and regulations undertaken by the FIU and supervisory organization in Luxembourg that are actively involved in the fight against ML/TF, shedding light on their important roles and contributions.

The Cellule de Renseignement Financier (CRF), Luxembourg's financial intelligence unit operating under a prosecutorial model, plays a crucial role in the country's AML/CFT framework as an autonomous entity led by independent magistrates.[136] This type of FIU is commonly found in countries with a continental law tradition, where the FIU is under the jurisdiction of the prosecutor's office or judicial system.[137]

As the primary intelligence and detection agency, the CRF is responsible for collecting and analyzing financial intelligence to combat ML/TF.[138] The national AML/CFT rules and regulations in Luxembourg grant magistrates the power to initiate analysis, bolstering the CRF's independence, investigative capabilities, agility, and comprehensive approach to combating money laundering and terrorist financing. These changes contribute to a more effective and proactive FIU, strengthening the overall AML/CFT efforts in Luxembourg.

---

[133] Jayesh D'Souza, *Terrorist Financing, Money Laundering and Tax Evasion- Examining the Performance of Financial Intelligence Unit* (Taylor & Francis Group, 2012) p. Xv

[134] Alhosani (n 131) p. 93

[135] Pieter Lagerwaard, 'Financial Surveillance and the role of the Financial Intelligence Unit (FIU) in the Netherlands' (2023) 26(7) Journal of Money Laundering Control p. 79

[136] Ministry of Justice of the Government of the Grand Duchy of Luxembourg, 'National Risk Assessment of Money Laundering and Terrorist Financing' (*Mj.gouvernement.lu*, 15 September 2020) <https://mj.gouvernement.lu/dam-assets/dossiers/blanchiment/en-nra-import-version-2982022.pdf> accessed on 1 July 2023 p. 154

[137] Schott (n 130) p. VII-13

[138] Ministry of Finance of the Luxembourg Government, 'International Financial Sanctions' (*Mfin.gouvernement.lu*) <https://mfin.gouvernement.lu/en/dossiers/2018/sanctions-financiaires-internationales.html> accessed on 5 July 2023.

The CRF serves as a key counterpart in national coordination efforts to combat financial crimes. It collaborates closely with other domestic law enforcement agencies, regulatory bodies, and international FIUs, facilitating the exchange of information and intelligence. This close collaboration enhances the effectiveness of investigations and prosecution of ML/TF cases.

On the other hand, the Commission de Surveillance du Secteur Financier (CSSF) is the prudential and AML/CFT supervisory authority in Luxembourg's financial sector. Its role is to oversee and supervise various financial sector professionals, including banks, EMIs, payment institutions, investment firms, collective investments, and market operators.

The CSSF plays critical role in the preventive part of ML/TF, ensuring that these OEs comply with AML/CFT regulations and implement effective measures.[139] It provides guidance, regulations, and conducts inspections to evaluate the adequacy of the AML/CFT frameworks and controls in place within the supervised entities. The relation between the CRF and the CSSF is characterized by close cooperation and coordination. Both institutions work hand in hand to combat ML/TF effectively. They exchange information, share intelligence, and collaborate on initiatives aimed at strengthening the AML/CFT framework in Luxembourg's financial sector. This collaborative approach ensures a comprehensive and integrated effort to detect, prevent, and prosecute financial crimes. By combining the financial intelligence expertise of the CRF with the supervisory oversight of the CSSF, Luxembourg enhances its ability to combat ML/TF and maintain the integrity of its financial system.

5. CONCLUSIONS

The present study delved into the intricate relationship between ML and e-money and the role of EMIs in combating ML/TF within the framework of the European Union.

As illicit activities continue to pose significant threats to European and global financial stability, the emergence of e-money has introduced new challenges to effectively combat money laundering. This conclusion highlights the key findings and implications drawn from the research conducted in the preceding chapters.

The study began with by elucidating the concept of e-money and the regulatory structure of e-money rules and regulations within the European Union. These regulatory

[139] CSSF, 'FAQ regarding the fight against money laundering and terrorist financing (AML/CFT) for individuals/investors' (*Cssf.lu*, 4 June 2021) <https://www.cssf.lu/wp-content/uploads/FAQ_AMLCTF.pdf> accessed on 10 July 2023 p. 11

developments unveiled the advancements in e-money operations and the benefits it brings to financial transactions. However, this study also shed light on the potential vulnerabilities of e-money systems to exploitation for money laundering purposes. It further underscored the significance of establishing robust regulatory frameworks to maintain the integrity of electronic payment systems and mitigate potential risks associated with ML.

In order to have better understanding of the role of EU EMIs in combating ML/TF, the study also elaborated the concept of money laundering as the process of legitimizing unlawfully acquired funds and assets, emphasizing its association with illegal activities such as drug trafficking, arms smuggling, human trafficking, and terrorism financing. ML comprises three stages: placement by moving illegal funds into the legitimate system, layering by concealing the trail, and integration by cleansing illegal funds which appear legitimate in the financial system. The gravity of this issue has led to its recognition as a substantial global threat, necessitating a multi-dimensional approach to counteract its pervasive effects.

The investigation into the relationship between ML and e-money revealed the potential misuse of e-money for illicit activities. The study identified various money laundering techniques that exploit the features of electronic money, necessitating a comprehensive understanding of these methods to effectively combat such criminal activities. Electronic Money Institutions play a crucial role in the fight against ML/TF. Accordingly, EMIs should designate a compliance officer and offer regular AML training to all employees. It is essential to foster a strong compliance culture within the EMI and extend it to all branches and subsidiaries. Implementing continuous monitoring of suspicious activities, maintaining thorough record-keeping practices, and adopting a robust KYC process based on a risk-based approach are crucial for EMIs. This thesis recognized the significance of implementing these stringent measures and precautionary practices within EMIs to identify and thwart potential money laundering attempts involving electronic money. By actively participating in combating illicit activities, EMIs can contribute to preserving EU financial system integrity and safeguarding societal well-being.

In conclusion, the study underscores the urgency and importance of adopting a proactive stance against money laundering in the digital age. As electronic money gains momentum, so do the possibilities for its misuse in illegal financial activities. The EU regulators must continue to devise comprehensive strategies, regulations, and measures to ensure the secure and legitimate usage of electronic money while thwarting any attempts to exploit it for illicit purposes. Further, the most difficult but importantly, practical, and efficient risk-based approach must be developed among all obliged and governmental entities.[140] The combat against ML is impeded by diverging interpretations and fragmented application of AML/CFT rules among the Member States. Inconsistencies in how these rules are understood and implemented create complexities and challenges in effectively tackling the global issue of ML. By promoting collaboration and harmonized approach to AML/CFT regulations between regulatory bodies, financial institutions, and Electronic Money Institutions, the fight against ML can be strengthened. Enhanced information sharing, vigilance in monitoring transactions, and continuous advancements in technology will undoubtedly contribute to a safer and more transparent financial landscape. Ultimately, the role and obligations of EMIs in preventing financing of criminal activities and ML are pivotal in upholding the integrity of the financial system and maintaining a safe and secure environment for all stakeholders. By adhering to these stringent EU AML regulations, EMIs contribute significantly to the collective effort of combating illicit financial activities and preserving the trust of customers and the broader society in electronic money services.

[140] Martin Gill & Geoff Taylor, 'Preventing Money Laundering or Obstructing Business: Financial Companies' Perspectives on Know Your Customer Procedures' (2004) 44 Brit J Criminology 582 p. 593

BIBLIOGRAPHY

Legislations, Protocols

1. Consolidated Version of the Council Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L267/7
2. Consolidated Version of the Council Directive 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L141/73
3. Consolidated Version of the Council Directive 2015/2366 of 25 November 2015 on payment services in the internal market amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35
4. Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information [2000] OJ L271
5. Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering [1991] OJ L166
6. Council Directive 2000/46/EC of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions [2000] OJ L275/39
7. Council Directive 2001/97/EC of 4 December 2001amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering [2001] OJ L344
8. Council Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing [2005] OJ L309/15
9. Council Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions (recast), OJ L 177

10. Council Directive 2018/843 of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43
11. United Nations, 'United Nations Convention against Transnational Organized Crime and the Protocols Thereto' (2004)

Recommendations, Proposals, Opinions and Reports

1. European Banking Authority, 'Opinion on Money Laundering and Terrorist Financing Risks Affecting the EU Financial Sector' (3 March 2021) EBA/Op/2021/04
2. European Banking Authority, 'Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)' (23 June 2022) EBA/Op/2022/06
3. European Banking Authority, 'Opinion on Money Laundering and Terrorist Financing Risks Affecting The EU's Financial Sector' (13 July 2023) EBA/Op/2023/08
4. European Central Bank, Report on Electronic Money (August 1988)
5. European Central Bank, 'Opinion of the European Central Bank of 16 February 2022 on a proposal for a regulation establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism' (2022) C 210/05
6. European Commission, 'Report from the Commission to the European Parliament and the Council on the implementation and impact of Directive 2009/110/EC in particular on the application of prudential requirements for electronic money institutions' (2018) COM/2018/041 final
7. European Commission, 'Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market relating to cross-border activities' (2022) COM/2022/554 final
8. European Commission, 'Proposal for a Directive of the European Parliament and of the Council of on the taking up, pursuit and prudential supervision of the business of electronic money institutions, amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC' (2008) COM/2008/0627 final
9. European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing' (2021) COM 420 final

10. European Commission, 'Proposal for a Regulation of the European Parliament and of the Council establishing the European Authority for Countering Money Laundering and Financing of Terrorism, amending Regulations (EU) No 1093/2010 (EU) 1094/2010 and (EU) 1095/2010' (2021) COM 421 final
11. European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets' (2021) COM 422 final
12. European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the mechanisms for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849' (2021) COM 423 final
13. European Commission, 'Communication from the Commission to the European Parliament and the Council towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework' (2019) COM 360 final
14. European Commission, 'Communication from the Commission to the European Parliament and the Council on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing' (2020) C 164/21
15. FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF Recommendations' (updated February 2023) <https://www.fatf-gafi.org/content/dam/recommandations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf> accessed on 23 March 2023

Academic Sources

1. Alhosani W, *Anti-Money Laundering: A Comparative and Critical Analysis of the UK and UAE's Financial Intelligence Units* (Palgrave Macmillan UK 2016)
2. Allegrezza S, 'The proposed Anti-Money Laundering Authority, FIU cooperation, powers and exchanges of information: A Critical Assessment' (July 2022) Publication for the committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.
3. Amrani H, 'The Development of Anti-money Laundering Regime: Challenging Issues to Sovereignty, Jurisdiction, Law Enforcement, and Their Implications on the Effectiveness in Countering Money Laundering' (Doctoral thesis, Erasmus University Rotterdam 2012)

4. Athanassiou P, Mas-Guix N, ‘Electronic Money Institutions Current Trends, Regulatory Issues and Future Prospects’ (July 2008) 7 European Central Bank Legal Working Paper Series
5. Cox D, *Handbook of Anti Money Laundering* (John Wiley & Sons 2014)
6. Dunfee T, Baker C, ‘Review: The Impact of Dirty Money on Global Capitalism’ (2007) 17(4) Business Ethics Quarterly
7. D'Souza J, *Terrorist Financing, Money Laundering And Tax Evasion: Examining The Performance Of Financial Intelligence Units* (CRC Press 2011)
8. D'Souza J, *Terrorist Financing, Money Laundering and Tax Evasion- Examining the Performance of Financial Intelligence Unit* (Taylor & Francis Group 2012)
9. Ehrlich T, ‘To Regulate or Not - Managing the Risks of E-Money and Its Potential Application in Money Laundering Schemes’ (1998) 11 Harv J L & Tech 833
10. Fratangelo P, *The New Anti-Money Laundering Law: First Perspectives on the 4th European Union Directive* (Palgrave Macmillan 2016)
11. Gill M, Taylor G, ‘Preventing Money Laundering or Obstructing Business: Financial Companies' Perspectives on Know Your Customer Procedures’ (2004) 44 Brit J Criminology 582
12. Halpin R, Moore R, ‘Developments in electronic money regulation – the Electronic Money Directive: A better deal for e-money issuers?’ (2009) 25 Computer Law & Security Review
13. Ioannides E, *Fundamental Principles of EU Law Against Money Laundering* (Ashgate Publishing Company 2014)
14. Janson N, ‘The Development of Electronic Money: Toward the privatization of money issue?’ (2004) 9(2) Journal of Internet Banking and Commerce
15. Krueger M, ‘E-money regulation in the EU’ in Robert Pringle and Matthew Robinson (eds), *E-Money and Payment Systems Review* (Central Banking 2002)
16. Lagerwaard P, ‘Financial Surveillance and the role of the Financial Intelligence Unit (FIU) in the Netherlands’ (2023) 26(7) Journal of Money Laundering Control
17. Levi M, *Money Laundering: Risks and Countermeasures* (Australian Institute of Criminology 1996)
18. Loesch S, *A Guide to Financial Regulation for Fintech Entrepreneurs* (John Wiley & Sons Incorporated 2018)
19. Magliveras K, ‘The European Community’s Combat Against Money Laundering: Analysis and Evaluation’ (1998) 5 ILSA Journal of International & Comparative Law

20. Mitsilegas V, Gilmore B, ‘The EU Legislative Framework Against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards’ (January 2007) 56 International and Comparative Law Quarterly
21. Mugarura N, ‘Customer Due Diligence (CDD) Mandate and the Propensity of its Application as a Global AML Paradigm’ (2014) 17(1) Journal of Money Laundering Control
22. Murphy C, *EU Counter-Terrorism Law : pre-emption and the rule of law* (Hart Publishing 2015)
23. Pavone P, Parisi F, ‘Compliance and Corporate Anti-Money Laundering Regulation’ (2018) 7(2) Journal of Governance and Regulation
24. Rajput V, ‘Research on Know Your Customer (KYC)’ (2013) 3 International Journal of Scientific and Research Publications
25. Reuter P, Truman E, *Chasing Dirty Money: The fight Against Money Laundering* (Peterson Institute for International Economics 2004)
26. Samantha A, Irwin M, Choo K, ‘An analysis of money laundering and terrorism financing typologies’ (December 2011) 15(1) Journal of Money Laundering Control
27. Schott P, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (2. World Bank Publications 2006)
28. Silva P, ‘Recent developments in EU legislation on anti-money laundering and terrorist financing’ (2019) 10(1) New Journal of European Criminal Law
29. Straub J, ‘The Prevention of E-Money Laundering: Tracking the Elusive Audit Trail’ (2002) 25 Suffolk Transnat'l L Rev 515
30. Unger B & Den Hertog J, ‘Water always finds its way: Identifying new forms of money laundering’ (2012) 57 Crime L & Soc Change 287
31. Wilusz D, ‘Legal determinants of electronic money systems development in European Union’ (2011) 2 Pedrawny i ekonomiczny przegląd prawa gospodarczego Wydawnictwo Naukowe UAM
32. Woda K, ‘Money Laundering Techniques With Electronic Payment Systems’ (2006) 18 Information & Security Journal
33. Zachariadis M, Özcan P, ‘The API Economy and Digital Transformation in Financial Services: The Case of Open Banking’ (June 2017) Swift Institute Working Paper 2016-001 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975199 accessed on 24 March 2023

Other Documents and Web Sources

1. Bindseil U, Schneeberger D, 'Cash or cashless? How people pay' (*The ECB Blog*, 6 February 2023) <https://www.ecb.europa.eu/press/blog/date/2023/html/ecb.blog230206~1ea270a762.en.html> accessed on 10 February 2023
2. Central Bank of Bahrain, 'Combating the Financing of Terrorism Guidance for Financial Institutions', (*Cbb.gov.bh*, November 2020) <https://www.cbb.gov.bh/wp-content/uploads/2021/10/Guidance-Paper-Combating-the-Financing-of-Terrorism_17-Nov-2020.pdf> accessed on 20 March 2023
3. CSSF, 'FAQ regarding the fight against money laundering and terrorist financing (AML/CFT) for individuals/investors' (*Cssf.lu*, 4 June 2021) <https://www.cssf.lu/wp-content/uploads/FAQ_AMLCTF.pdf> accessed on 10 July 2023
4. De Best R, 'Number of e-money purchase transactions in the European Union from 2000 to 2021' (*Statista.com*, March 2023) <https://www.statista.com/statistics/443399/electronic-money-payment-in-european-union/> accessed on 24 March 2023
5. European Central Bank, 'Electronic Money' (*Ecb.europa.eu*) <https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html> accessed on 1 December 2022
6. European Commission, 'European Commission welcomes the European Parliament's adoption of two proposals in the area of payments (on e-money and cross-border payments)' (*Ec.europa.eu*, April 2009) <https://ec.europa.eu/commission/presscorner/detail/en/IP_09_637> accessed on 26 December 2022
7. European Commission, 'Commission presents Action Plan to strengthen the fight against terrorist financing' (*Ec.europa.eu*, 2 February 2016) <https://ec.europa.eu/commission/presscorner/detail/en/IP_16_202> accessed on 2 May 2023
8. European Commission, 'European Commissions – Infringement decisions' (*Ec.europa.eu*, April 2023) <https://ec.europa.eu/commission/presscorner/detail/en/inf_23_1808> accessed on 2 May 2023
9. European Council, 'Anti-money laundering: Council adopts rules which will make crypto-asset transfers traceable' (*Consilium.europa.eu*, 16 May 2023)

<https://www.consilium.europa.eu/en/press/press-releases/2023/05/16/anti-money-laundering-council-adopts-rules-which-will-make-crypto-asset-transfers-traceable/> accessed on 19 May 2023

10. European Parliament, 'Stopping the flow of dirty money: Parliament ready for negotiations' (*Europarl.europa.eu*, 19 April 2023) <https://www.europarl.europa.eu/news/en/press-room/20230414IPR80123/stopping-the-flow-of-dirty-money-parliament-ready-for-negotiations> accessed on 16 May 2023
11. European Union, 'Aims and Values' (*European-union.europa.eu*) <https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en#:~:text=achieve%20sustainable%20development%20based%20on,the%20quality%20of%20the%20environment> accessed on 1 May 2023
12. FATF, 'Professional Money Laundering' (26 July 2018) < https://www.fatf-gafi.org/en/publications/Methodsandtrends/Professional-money-laundering.html> accessed on 25 March 2023
13. FATF, 'What is Money Laundering?' (*Fatf-gafi.org*) <https://www.fatf-gafi.org/en/pages/frequently-asked-questions.html#tabs-36503a8663-item-6ff811783c-tab> accessed on 20 March 2023
14. Financial Crime Academy, 'The Three Stages of Money Laundering: The Characteristics of the Money Laundering Stages' (*Financialcrimeacademy.org*) <https://financialcrimeacademy.org/the-three-stages-of-money-laundering/> accessed on 2 April 2023
15. Group of Ten, 'Electronic Money: Consumer protection, law enforcement, supervisory and cross border issues' (*Bis.org*, April 1997) Bank for International Settlement <https://www.bis.org/publ/gten01.htm> accessed on 01 December 2022
16. Lagarde C, Panetta F, 'Key objectives of the digital euro' (*The ECB Blog*, 13 July 2022) <https://www.ecb.europa.eu/press/blog/date/2022/html/ecb.blog220713~34e21c3240.en.html> accessed on 10 February 2023
17. Ministry of Finance of the Luxembourg Government, 'International Financial Sanctions' (*Mfin.gouvernement.lu*) https://mfin.gouvernement.lu/en/dossiers/2018/sanctions-financiaires-internationales.html accessed on 5 July 2023
18. Ministry of Justice of the Government of the Grand Duchy of Luxembourg, 'National Risk Assessment of Money Laundering and Terrorist Financing' (*Mj.gouvernement.lu*, 15 September 2020) <https://mj.gouvernement.lu/dam-assets/dossiers/blanchiment/en-nra-import-version-2982022.pdf> accessed on 1 July 2023

19. Snoeck J, 'Ikea trials cashless store in the Netherlands' (*Retaildetail.eu*, 3 September 2019) <https://www.retaildetail.eu/news/home/ikea-trials-cashless-store-netherlands/> accessed on 10 February 2023
20. The World Bank, *Innovations in Retail Payments Worldwide: A Snapshot* (The World Bank 2012)
21. UNODC, 'Money Laundering' (*Unodc.org*, April 2018) <https://www.unodc.org/e4j/en/organized-crime/module-4/key-issues/money-laundering.html> accessed on 1 April 2023
22. U.S. Congress, Office of Technology Assessment, '*Information Technologies for the Control of Money Laundering*' (U.S. Government Printing Office September 1995)
23. Wahl T, 'AML Package III: 6th AML Directive Proposed' (*Eucrim.eu*, 5 August 2021) <https://eucrim.eu/news/aml-package-iii-6th-aml-directive-proposed/> accessed on 16 May 2023
24. 'Egmont Group of Financial Intelligence Units' (*Wikipedia*) <https://en.wikipedia.org/wiki/Egmont_Group_of_Financial_Intelligence_Units> accessed on 2 July 2023