University of Stavanger

ANJA BJØRNSBRÅTEN ILDJARNSTAD
SUPERVISOR: PROFESSOR ANDREA MINTO

The Changing Landscape of Customer Due Diligence in AML Legislation: Implications for Digital Onboarding and External Service Providers

Master thesis, 2023
Master of Business law
University of Stavanger Business School
Specialization: Business law
Words: 14 483

Universitetet i Stavanger

HANDELSHØGSKOLEN VED UIS

MASTEROPPGAVE

STUDIEPROGRAM: Master i Forretningsjus	OPPGAVEN ER SKREVET INNEN FØLGENDE SPESIALISERINGSRETNING: Forretningsjus ER OPPGAVEN KONFIDENSIELL? (**NB**! Bruk rødt skjema ved konfidensiell oppgave)

TITTEL:
Endringene i landskapet for kundekontroll i AML-lovgivning: Implikasjoner for digital onboarding og eksterne tjenesteleverandører

ENGELSK TITTEL:

The Changing Landscape of Customer Due Diligence in AML Legislation: Implications for Digital Onboarding and External Service Providers

FORFATTER(E)		VEILEDER:
Kandidatnummer: 3205 ……	Navn: Anja Bjørnsbråten Ildjarnstad ……	Professor Andrea Minto

Table of Contents

Abstract

Over the last decades, advancement in financial technology has led to a significant change in how financial institutions conduct customer due diligence (CDD) within anti-money laundering (AML) legislation. Technology has enabled digital onboarding and has made it easier for such institutions to verify their customer's identity and assess the risk of money laundering or terrorist financing. This has also led to increased outsourcing as most aspects happen digitally and has introduced new risks and concerns. In correspondence, the AML directives must also develop to regulate recent trends to prevent money laundering and terrorist financing. This thesis explores these new concerns and challenges concerning customer due diligence (CDD) within anti-money laundering (AML) legislation by focusing on digital onboarding and outsourcing to external service providers. It highlights the current AML framework and its efficiency, the advantages and disadvantages with onboarding, and risks associated with outsourcing CDD activities to external service providers.

List of Abbreviations

AML – Anti-Money Laundering

AML/CFT – Anti-Money Laundering and Countering the Financing of Terrorism

AMLA- Anti-Money Laundering Authority

AMLAR-Regulation establishing the Anti-Money Laundering Authority

AMLD- Anti-Money Laundering Directive

AMLD 1- First Anti-Money Laundering Directive

AMLD 2- Second Anti-Money Laundering Directive

AMLD 3- Third Anti-Money Laundering Directive

AMLD 4- Fourth Anti-Money Laundering Directive

AMLD 5- Fifth Anti-Money Laundering Directive

AMLD 6 – Sixth Anti-Money Laundering Directive

CTF - Counter-Terrorist Financing

CDD- Customer Due Diligence

EBA- European Banking Authority

ESA- European Supervisory Authority

EU- European Union

FATF-Financial Action Task Force

FATCA – Foreign Account Tax Compliance Act

TF- Terror Financing

Introduction

Financial technology is constantly under development and are getting more advanced. Digital onboarding and outsourcing of services are outcomes of such development. However, more advanced financial technology also represents a risk for regulations. This has prompted the European Union to reconsider its approach and adjust to these technological advancements when it comes to combating money laundering and terrorist financing (TF).[1] Further, financial development has the potential to make measures against money laundering and terrorist financing cheaper, faster, and more effective. New financial technology addresses financial instruments that are used by criminals to launder money and finance terrorism and others. However, there are also risks associated with financial technology; for instance, compliance with anti-money laundering legislation (AML) may, in many cases, remains inadequate. Thus, new financial technology forces the framework of AML to change simultaneously with the new financial technology evolution. In the fourth AML directive, 2015/849 the customer due diligence. Such as Know Your Customer (KYC) are stipulated under Article 13[2] and represents an important step in this direction.

The topic to be presented in this thesis is customer due diligence, also called CDD. With a focus on digital onboarding and outsourcing to external service providers to perform the different CDD activities. Onboarding new customers automatically triggers an AML and CTF obligation to conduct customer due diligence before establishing a relationship with the customers. More and more interactions with and recruitment of customers happen digitally. Thus, to ensure compliance with the AML legislation, companies must collect, verify, and regularly update information about their customers. Within CDD, there are four activities that those who are subject to the AML-legislation (obliged entities) need to follow. This is stipulated under Article in EU directive 2015/849. The four activities are as follows[3]: *1) Identifying the customer; 2) identifying the beneficial owner; 3) obtaining information; and 4) conducting ongoing monitoring of the business relationship.*

Money laundering is an increasing issue that follows financial technology development and has severe consequences. It is, therefore a demanding and serious task for obliged entities subject to the AML-legislation and CDD. Onboarding requires enormous resources from obliged entities. Especially as the difficulty of preventing and tracking money laundering

[1] EBA «Report on the use of digital platforms" (EBA/REP/2021/26) pg.12.
[2] Directive 2015/849/EU art. 13.
[3] Directive 2015/849/EU art. 13 (1) a-d.

increases with digitalization. Also, verifying that 20.000 customers are whom they claim to be is time-consuming. Consequently, obliged entities have been trying other ways to get around the responsibility of customer due diligence. This has led to outsourcing to external service providers, which introduced new concerns.

Today the AML-legislation is built up by five different AML-directives[4] to cover the fields of anti-money laundering and counter-terrorist financing. The directives evolve and changes intact with the evolution of AML and CTF. It is an important regulation because of the combating of AML and CTF, and the overall goal with such legislation is to prevent money laundering and also avoid that criminals that have committed a crime can make their money appear to be legal or that the laundered money is used to terrorist financing (TF).[5]

The lack of the current framework is that there today are different directives, and these need to be transposition into the different laws of each country. Since there is no familiar harmonization of the framework within the EU countries, this can lead to breaches between national supervisors and financial intelligence units.[6]

Further, this thesis will use a legal dogmatic perspective since the thesis will build up on systemizing, clarifying, and analysing the European anti-money laundering legislation, focusing on the relevant EU legislation and upcoming EU directive. The thesis will also include legal and political considerations regarding the challenges concerning CDD in anti-money laundering legislation.

This thesis will not examine case law, as there is none on this subject matter. If such precedents existed, they might have come from the European Court of Justice interpretation or national case law concerning Norwegian legislation transpiration and dispute relating to CDD and hereunder outsourcing. However, there are no current cases relating to this specific topic that are available for examination

In addition, legal sources will be considered, including how the subject matter will change over time from directive to regulation. Also, legislation such as hard and soft laws by the EBA and FATF will be presented and examined. As this thesis also focuses on developing on the legal framework, it will also consider some national legislation. Lastly, this thesis will also incorporate established literature on the subject matter. This includes books, academic

[4] AMLD 1:Directive 91/308/EEC, AMLD 2: Directive 2001/97/EC, AMLD 3: Directive 2005/60/EC, AMLD 4: Directive 2015/849, AMLD 5: Directive 2018/843/EU.
[5] Cox, Dennis. *Handbook of Anti Money Laundering* (England: Wiley, 2014), 15.
[6]European Commission, «Commission steps up against money laundering and terrorist financing" (report European Comission, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_800).

publications, and scholarly articles that consider and discuss the relevant legal theory and concepts related to AML and CDD.

This thesis aims to explore the new challenges concerning customer due diligence (CDD) in the anti-money laundering legislation (AML), with a focus on digital onboarding and outsourcing to external service providers. To accomplish this, three sub-questions will be discussed and answered throughout three different chapters. The following sub-questions are:

1. The current state and efficiency of customer due diligence (CDD) within Anti-money laundering legislation (AML)
2. What are the advantages and disadvantages of digital onboarding in Customer Due Diligence (CDD) in Anti-Money Laundering (AML) legislation, and are there any risks associated with this process?
3. What are the risks associated with outsourcing of customer due diligence (CDD) processes to external service providers, and are there any advantages and disadvantages of outsourcing to external service providers for CDD requirements in AML legislation?

Chapter 1 of the thesis will focus on the AML-framework and CDD. With given definition on both anti-money laundering (AML) and counter-terrorism (CT). A presentation of the Financial Action Task Force (FATF) and an introduction on soft law will be given. Leading to an overview of legislation, both European and domestic, with a focus on hard law, this is to show the current state and efficiency of the AML legislation and hereunder CDD. The chapter will discuss the increase of digitalization, such as new virtual currencies. Lastly, critical legal issues with the current framework will be presented.

In chapter 2 of the thesis, the focus will be on digital onboarding and a definition on digital onboarding will be given, and also the development of CDD will be presented. Both hard law and soft law within onboarding and CDD will be analyzed. Further, the different risks associated with onboarding will be explored.

Chapter 3 will then consist of an analysis of outsourcing to external service providers, with both hard laws from section IV of the AMLD 4 and soft law from both FATF and the EBA. Further, the chapter will consist of the upcoming reform (AMLD 6) focusing on outsourcing to external service providers. Lastly, this chapter will explore risks with outsourcing.

Finally, the concluding chapter will provide a summary on the analysis throughout the three chapters and will also answer the three given sub-question, this to accomplish the aim of the thesis.

Chapter I: AML and CDD: State of the current framework

1.1Introduction

First in this chapter, a definition on anti-money laundering (AML) and counter-terrorist financing (CTF) will be given. This will provide an overall explanation of the process of both AML and CTF. Second, the important role of the Financial Action Task Force (FATF) in both combating of money laundering, and terrorist financing and proliferation financing will be presented. Thirdly, the legal perspective will be separated in to two parts. The first part will focus upon the European perspective on AML-legislation and developments. Further, the second part will address the domestic perspective, hereunder the Norwegian legislation on AML, with the focus on customer due diligence in the Norwegian framework. Then back to the overall picture with the different AML-directives from 1991-2018 and ending with the proposal for an upcoming AML-directive with its six pillars. Also, CDD in AML-legislation will be presented. Lastly, the chapter concludes by going through different critical legal issues of the current regulatory aml-framework.

1.2 Definition of Money Laundering and Counter-Terrorism

Money laundering is defined by Directive 2015/849/EU (commonly referred to as 4th AMLD). Namely, article 1(3) under letter a through d reads as follow: [7] "*the following conduct, when committed intentionally, shall be regarded as money laundering:*

a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action

b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity

c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity

[7] Directive 2015/849/EU art. 1 (3).

d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c"

The overall goal of AML and CTF is to both combat and prevent money laundering from performed crimes, and combat and prevent that laundered money can be used to finance terrorism. Further, the rules within AML includes financial and admirative provisions and the aim of AML is to uncover activities of money laundering.[8] Money laundering can be funds that are tried to be laundered and they can have origin from theft, corruption, tax evasion, fraud, and sale of drugs. Such funds from a money laundering process comes from criminal activities and are so-called second-degree felonies.

1.2.1 Money Laundering

There are three stages in the money laundering process: placement, layering and integration.[9] Firstly, the placement stage starts with the funds originating from illegal criminal activities such as drug trafficking, theft, or other form of criminal activities. In the process of making the funding legal, the illegal funds need to be put into the banking system without raising suspicion and also to hide the illegal origin of the funds. Furthermore, the illegal funds need to be laundered so they can be used without getting caught and punished for how they got the funds in their possession. This can be done by shifting the funds from their original form into another form. Within the placement stage different placements or purchases can be used, some of them is purchase things in the marked, purchase of antiques, investing in different investment products, purchase of boats, buying chips at a casino or lottery tickets, or giving out cash loans to example private companies and more.[10] An example of money laundering is using the illegal fund from criminal activities to purchase an item such as antiques. When selling the obtained antiques, the criminal funds will be "legitimate" because the sale of the antiques will make the illegal money appear to originate from legal activities. This is the first stage of money laundering, after hiding where the funds originate from there is the layering stage.

[8] Rui, *Hvitvasking* (Oslo: Universitetsforlaget, 2012), 25.
[9] Cox, Dennis. *Handbook of Anti Money Laundering* (England: Wiley, 2014), 15.
[10] Cox, Dennis. *Handbook of Anti Money Laundering* (England: Wiley, 2014), 16.

The overall aim of the layering stage is to cover up that the funds are originating from something illegal. This is done by using the illegal funds to purchase and invest in products that is legal. By laundering money through legal channels, the money launderers make it harder to track down and uncover illegal funds.[11] An example is buying and renovating a house with funds originating from the criminal activities. The criminal funds will appear legitimate when the renovation is finished, or when the house is sold because selling the house releases new funds. Since obtaining real estate often involves a solicitor or a layer it is more difficult to successfully launder money this way. Moreover, someone who is selling property is an obliged entity under AML-legislation[12], this can make the obliged entity legally bound to obtain both information of the customer and the origin of the funds, cf. art 2 cf. art 13[13] and other information regarding due diligence of a customer. The example of antiques given in the placement stage can also be used for the layering stage, because antiques can be obtained in various ways. For example, by going into a flee marked, auctions or other stores and by the antique, but also by inherited from someone or maybe as a gift from someone. The different ways of obtaining different antique items is making the origin of the funds harder to trace and verify. As a result of both the placement and the layering stage the funds from the criminal activity can now appear as originate from legal channels.

The Integration/extraction stage is the last stage in the laundering process. Here the illegal funds are being disguised into the financial system so they can appear to be legitimate funds. The goal in this process is to make the funds so legitimate that it is almost impossible to separate the illegal funds from the legal funds.[14] Through holding and securing different objects, the money launderers can take them to use and launder their illegal funds. Additionally, money launderers can obtain such items with the laundered money, and this can be used to buy items and different type of services like art, property, cars, and other items.

[11] J. C. Sharman. *The Money Laundry*. (1st ed. Cornell University Press, 2011), 15-16.
[12] Directive 2015/849/EU art. 2 letter b.
[13] Directive 2015/849/EU art.2 and art. 13.
[14] Cox, Dennis. *Handbook of Anti Money Laundering* (England: Wiley, 2014), 18-20.

1.2.2 Terrorist Financing

Terrorist financing (TF) is defined in article 1 (5) of the AML-directive as: [15] *the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA.* Further, a definition is also given in the terror financing risk assessment guidance from FATF, and in the same guidance FATF also includes TF threats such as both international and domestic terrorist organizations and hereunder their funds, supporters, helpers but also single population or groups of people that are sympathetic towards the different terrorist organizations.[16]

Since 2001 CTF have been under priority from FATF and CTF was also added under the third AML-directive.[17] TF has also a process similar to the three stages of the money laundering process. TF has four different stages: Raise, store, move and use.[18]

1.3 The Financial Action Task Force

In the current AML framework, the Financial Action Task Force (FATF) has an important role. FATF was established in 1989 and has the purpose of combating money laundering, terrorist financing and proliferation financing.[19] Since the FATF recommendations are so called "soft law" instruments, the recommendations are not binding. Despite this, FATF is still important when it comes to combating money laundering and terrorist financing. One of the tasks of FATF is to ensure that different countries are implementing the FATF standards, both effectively and fully.[20] Also, FATF can hold countries accountable if they do not follow the implementations of the FATF standards. This can also be seen in the FATF: Consolidated Processes and Procedures for Mutual Evaluations and Follow-Up, "Universal Procedures" from

[15] Directive 2015/849/EU art. 1 paragraph 5.
[16] FATF Recommendations "Terrorist Financing Risk Assessment Guidance" pg. 8, FATF, 2019, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Terrorist-financing-risk-assessment-guidance.html.
[17] Directive 2005/60/EC.
[18] United Nations office on Drugs and crime, "money Laundering" United Nations Office on Drugs and Crime, 2023, https://www.unodc.org/unodc/en/money-laundering/overview.html.

[19] FATF Recommendations "International standards on combating money laundering and the financing of terrorism & proliferation of weapons of mass destruction" https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

[20] FAFT, "What we do" https://www.fatf-gafi.org/en/the-fatf/what-we-do.html.

September 2022.[21] Here FATF updated to take into consideration for new initiatives that is not proper implemented by the national competent authority.

As earlier mentioned FATF comes up with recommendations and standards on matters when it comes to AML and CTF. Most recently FATF have presented some guidance and overall soft law that is stressing the riskiness of crypto and remote onboarding.[22] In the next two chapters the thesis will go deeper into the riskiness, disadvantages but also advantages when it comes to digital onboarding and outsourcing in customer due diligence (CDD) in anti-money laundering (AML) legislation.

1.4 The Relevance of Soft Law

The relevance of soft law is important for the law-making process and the process of documents such as guidance. Since the development of technology leads to outscoring for an easier customer establishment within the financial sector the need for guidance and recommendations on the matter of CDD is important. This is where the soft law such as recommendations by FATF and guidance from EBA, gives the legislator a guidance for further development of the AML-directives.

EBA are using the soft law through different guidelines and warnings. Also, EBA have introduced a guidance on the remote onboarding.[23] The increase of customer relationship established digital and through digital onboarding has developed over the years. Especially during the COVID-19 pandemic and this also underlined the importance of an institutions having effective means to comply with the CDD requirements within the AML-legislation.[24] Further, the importance when it comes to soft law in both digital onboarding and outsourcing of activities within CDD will be highlighted in the next chapters of the thesis.

[21] FATF Recommendations Consolidated Processes and Procedures for Mutual Evaluations and Follow-Up "Universal Procedures" https://www.fatf-gafi.org/en/publications/Fatfgeneral/Universal-procedures.html.
[22] FATF, "Updated Guidance for a Risk-Based Approach to Virtual Asset Service Providers" https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html.
FATF " Guidance for a risk-based approach. The banking sector"(https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Risk-based-approach-banking-sector.html).
[23] EBA, Final report "Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849" (EBA/GL/2022/2015).
[24] EBA, Final report "Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849" (EBA/GL/2022/2015) pg.4.

1.5 European Perspective: The European Jurisdiction on AML

The European perspective has evolved and have been developed under the different AML-directives. In 1991, the first binding law on AML was founded as Directive 91/308/EEC "on the prevention of the use of the financial system for the purpose of money laundering". In this first directive the obliged entities were only credit and financial institutions, cf article 1.[25] This was also the start of customer identification which was stipulated under article 3 of the directive. The AML-directive from 2001, Directive 2001/97/EC extended beyond both credit and financial institutions, cf. article 2 such that lawyers that were managing the property and money for their clients was now included as obliged entities.[26] The first two directives were different from the later AML-directives, and the earlies directives only included the identification of the customer and not the later established due diligence. The evolution of money laundering led to the establishment of not only identification of the customer, but also due diligence. This was stipulated in the third directive, Directive 2006/70/EC "on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing". The third directive established due diligence under article 8: [27] *A- d. a) Identifying the customer. Meaning checking the identity from a secure source; b) benefiting from transaction behind the transaction. Is the person the one that benefits from the transactions. Meaning who is the beneficial owner; c) Obtaining information; d) Ongoing monitoring. Meaning that the obligation does not end when the relationship starts*. In later years the evolution of ways to launder money led to an extension of the obliged entities. In the fourth directive from 2015 both providers of gambling services and tax crimes were updated under article 2 of the directive.[28] The technology had developed further, and by the fifth directive the use of crypto currency was included.[29] Therefore, in the fifth directive, the list of obliged entities was updated to included crypto currency service providers.[30] The directive also gave and definition of crypto currencies and Article 3(1)(18) of AML directive from 2015 was amended in the directive from 2018, now including crypto currencies. The AML framework are still undergoing new reforms and are under proposal for a regulation in the prevention of anti-money

[25] Directive 91/308/EEC art. 1.
[26] Directive 2001/97/EC art. 2.
[27] Directive 2006/70/EC article 8.
[28] Directive 2015/849/EC article 2 on obliged entities .
[29] Gál, István László. "The 2018/843 Eu Directive on the Prevention of Money Laundering and Terrorist Financing and Its Correlation to the Criminal Law Prevention of the Stock Markets.", 116.
[30] Directive 2018/843/EC.

laundering authority and financing of terrorism, cf. COM (2021) 421 Final and the development of a new anti-money laundering directive.

1.5.1 Domestic perspective: The Norwegian Jurisdiction on AML

The Norwegian jurisdiction on AML is called *Act relating to measures to Combat Money Laundering and Terrorist Financing (the Anti-Money Laundering Act)*[31], but a definition on AML is given in the Norwegian Penal code law. Hereunder section 337 through 340 for money laundering and section 135 for Terrorist financing.[32] Further, the purpose of the legislation is given in section 1[33]:

1) The purpose of the Act is to prevent and detect money laundering and terrorist financing.

(2) The measures in the Act shall protect the financial and economic system, as well as society as a whole, by preventing and detecting the use or attempted use of obliged entities for purposes of money laundering or terrorist financing

The section of the Norwegian AML jurisdiction has the same purpose has the rest AML-directives such as AMLD 4. Hereunder, the overall purpose is to both prevent, uncover, and detect activities of money laundering and terrorist financing.

Furthermore, CDD and the measures to carry out CDD is laid down in §10 letter a to c.[34] After letter a, the measures for customer shall carry out when the *customer relationship is established*. Further, in letter b, CDD shall carry out for *transaction over (1) NOK 100.00 (2) NOK 8.000 and this if the transaction constitutes a transfer of funds as further defined by the ministry in regulations (3). NOK 16.00 for obliged entities, cf section 4, paragraph 2, letter g*. At last, letter c, CDD shall carry out in cases of *suspicion of money laundering or terrorist*

[31] Law 01. June 2018 no.23 Act relating to Measures to Combat Money Laundering and Terrorist Financing (the Anti-Money Laundering act) https://lovdata.no/pro/#document/NLE/lov/2018-06-01-23.
[32] Law 20. May 2005 no. 28 The penal code https://lovdata.no/pro/#document/NLE/lov/2005-05-20-28 ,Section 135 and 337.
[33] Act relating to Measures to Combat Money Laundering and Terrorist Financing (the Anti-Money Laundering act), section 1.
[34] Act relating to Measures to Combat Money Laundering and Terrorist Financing (the Anti-Money Laundering act) Section 10 (1) a-c.

financing.[35] Also, CDD shall be set in motion before transaction are being done or before the customer relationship are established.[36]

The identification of the customer as well as the identifying the beneficial owner, cf. Directive 2015/849 article 13 is similar to the Norwegian legislation on AML. In fact, the Norwegian Financial Supervisory Authority clarifies what the different alternatives for valid identification for a natural person[37]. Further, the list of required valid identification includes: *Norwegian and foreign passport, Norwegian driver license, Norwegian bankcard with picture, Norwegian identify card and other national identify card provided by another EEA[38], country Norwegian passport for foreigner, Norwegian travel document for refugees and electronic identification after the Norwegian AML-regulation section 4-3(4).[39]*

CDD and ongoing monitoring is stipulated under chapter 4, through section 9 to 24. Such as when the person is a natural person it is undergoing section 12 and if it is not a natural person it is under section 13.

The outsourcing of CDD measures are stipulated under section 23. Formerly, the terms for an outsourcing agreement is set under (2) of the article, and one of them is that the agreement shall be put into writing and also the obliged entity need to validate that the outsourcing service providers has the capacity and ability to carry out the requested outsourcing for their different customers. Further, the obliged entities under the Norwegian AML-Act are listed under section 4 and is the following legal entities[40]:

a. *banks;*
b. *credit institutions;*
c. *financing institutions;*
d. *Norges Bank [the central bank of Norway];*
e. *e-money institutions;*
f. *undertakings engaged in foreign exchange activities;*

[35] Law 01. June 2018 no.23 Act relating to Measures to Combat Money Laundering and Terrorist Financing (the Anti-Money Laundering act) Section 10 (1) a-c.
[36] Act relating to Measures to Combat Money Laundering and Terrorist Financing (the Anti-Money Laundering act), section 11.
[37] Finanstilsynet, «Hvitvaskingsregelverket og gyldig legitimasjon», *Finanstilsynet* https://www.finanstilsynet.no/tema/hvitvasking-og-terrorfinansiering/hvitvaskingsregelverket-og-krav-til-gyldig-legitimasjon/
[38] Forskrift 23. februar 2020, nr. 184 om endring i utlendingsforskriften (Vedlegg 4) https://lovdata.no/dokument/LTI/forskrift/2020-02-24-185
[39] Forskrift 01. Januar 2023, nr. 1960 forskrift om endring i forskrift om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsforskriften) https://lovdata.no/pro/#document/SF/forskrift/2022-11-15-1960?from=NL/lov/2018-06-01-23/
[40] Act relating to Measures to Combat Money Laundering and Terrorist Financing (the Anti-Money Laundering act), Obliged entities. Section 4(1) letter a – o.

g. *payment service undertakings and others entitled to provide payment services;*
h. *investment firms;*
i. *management companies for securities funds;*
j. *insurance undertakings;*
k. *undertakings engaged in insurance mediation that is not reinsurance broking;*
l. *central securities depositories, in cases where the central securities depository does not use an external account operator which is an obliged entity. For accountholders and issuers with an external account operator which is an obliged entity, such account operator is the obliged entity;*
m. *undertakings engaged in deposit activities;*
n. *managers of alternative investment funds;*
o. *loan mediation undertakings*

In the beginning of this year a new version of the Financial Agreement Act was updated and set into place.[41] This new law will in, for example fraud, give the customer better protection and this is one of the purposes of the legislation. Furtherly, the financial institutions commitment is getting more important, now it is important that the customer really understand the terms and condition of the agreement that they have with their financial institution, this is to ensure a balance between the customer and the different service providers of financial services.[42]

Økokrim is the main special body when it comes to investigating and prosecuting the ongoing financial crimes of AML and CTF in Norway.[43] The main goal is to combat economic crimes such as money laundering and terrorist financing but also environmental crimes. Since economic crimes also happens on a global basis the organization also collaborate globally. FATF, as earlier mentioned is one of the organizations that Økokrim cooperates with. Others organization can be both national organizations and hereunder the Norwegian Financial supervisory authority. Moreover, another globally organization that Økokrim collaborates with is the Foreign Account Tax Compliance Act (FACTA).[44]

[41] Law 18. December no. 146 Financial Agreements Act
https://lovdata.no/pro/#document/NL/lov/2020-12-18-146
[42] Prop.92 LS(2019-2020), pg. 10.
[43] Økokrim.no, «ofte stilte spørsmål» https://www.okokrim.no/ofte-stilte-spoersmaal.549336.no.html
[44] Gottschalk, Petter, and Ove Olsen. *Økonomisk Kriminalitet.*(Oslo: Cappelen Damm Akademisk, 2016), 375.

1.6 Upcoming Reform of the EU AML Regime

The European commission has proposed a new legislative reform with the aim of strengthening the AML/CTF framework. In 2019, the European Commission analyzed the AML/CTF framework and concluded that a reform was necessary[45]. The upcoming reform takes up the questions and warnings raised over the past few years by authorities and aim to provide systematic answers to the new market dynamics.[46] Further, on 7 May 2020 a proposal set by the European Commission introduced six priorities[47] to enhance the implementation and coordination of AML/CTF rules. Based on this the European Commission on the 20 of July presented a proposal for a new reform for AML/CTF legislation.[48] The six priorities are as follows:

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

2. Establishing an EU single rulebook on AML/CFT,

3. Bringing about 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."

As listed under priority 2 in the proposal, one of the initiatives behind this new reform is to develop all the current and future AML requirements from a directive towards a regulation. This, finally leading to the same set of rules for every member state. The new reform takes also another challenge into consideration, digital onboarding and outsourcing to external services providers within CDD. Today, obliged entities outsource their responsibility within CDD-activities to other obliged entities, which involves delegating task to qualified parties.

[45] SWD (2019) 650 final,COM(2019)371 final, COM (2019) 372 final, COM (2019) 373 final.
[46] Minto, Andrea""I'd love to help you, but I simply can't... or can I?" Anti-Money Laundering legislation and regulatory challenges concerning customer due diligence obligations in the platform era" pg. 11.
[47] COM (2021) 420 final "1. Context of the proposal".
[48] COM (2021) 420 final.

However, the proposal for AMLD 6 have evolved into outsourcing these responsibilities within CDD-activities to external service providers who are not necessary considered obliged entities.

1.7 CDD in AML-Legislation

Customer due diligence, hereafter referred to as CDD was presented in the fourth AML-directive, 2015/849. Article 13 of the directive stipulates CDD as well as KYC, and the article is an important step to combat money laundering. This due to the constant monitoring of the customer, not just when the relationship is established but also throughout the entire relationship between the beneficial owner and the customer. It is obliged entities that need to follow the activities set out under article 13, and different obliged entities are stipulated under aml-directive article 2. Hereunder credit institution cf. art 2(1)(1), financial institutions cf. art 2(1)(2) and others under art 2 (3).

Further, the different companies underlying the AML-directive needs to ensure that the legislation is being complied. In order to do so the obliged entities need to collect, verify and update the information about their customers. This is also stipulated under article 13.[49] The four activities that needs to be followed are: *(a) Identifying the customer: (b)Identifying the beneficial owner; (c) Obtaining information; and (d) Conducting ongoing monitoring of business relationship.*

Firstly, Letter a under article 13(1) commits the obliged entity to obtain information about their customer such as verification. The obliged entities also need to make sure that the collecting and verification of the identity comes from a reliable, independent and secure source. This can for example be done by collecting their full name, address, phone number, passport or other documentation that can verify the customer.

Secondly, Letter b under article 13(1) states that the obliged entities need to identify the beneficial owner. Meaning the real owner and finding out whether the customer is who they claim to be. Also, overall that the obliged entities need to check the identity of the person who wants to engage in a transaction.

Moreover, obliged entities need to obtain information about their customer, cf. article 13(1) letter c. This is so the AML-legislation can be complied with, and so suspicious transaction can be reported and followed up by the different obliged entities.

[49] Directive 2015/849/EU art. 13 (1) a-c.

At last, Letter d under article 13(1) makes sure that obliged entities conduct *"ongoing monitoring of business relationship".* In order for the obliged entities to comply with given AML-legislation the obliged entities need to monitor the relationship with their customer. This means that the obliged entities obligation does not end when the customer relationship starts. It also means that the obliged entities need to put in some effort when it comes to understanding the behavior of their customers. An example of this is KYC, where obliged entities, such as banks use this to collect and monitor the business relationship with their customer. The customer needs to fill in a form (either electronic- pr. Phone, computer and tablet or by post) stating their purpose with the business relationship. This can be stating their income, the origin of their funds, and other answers about their financials.

1.8 The Increase of Digitalization

New evolvement of technology as led to both solutions on the compliance of AML-legislation but also challenges when it comes to new currencies such as crypto.[50]

For example, FATF issued a *report about virtual currencies and the potential risk within AML/CTF*.[51] Some of the potential risk that FATF came up with in this report was the anonymity of transactions when using virtual currencies. Such transactions are not done in-person so you can not physically see the person that are performing the transaction, this is also making it difficult to verify the identity of the person who are sending and receiving the money. Further, such use of virtual currencies opens up for anonymous transactions, this makes the origin of the funds hard to track then other methods of payment, such as cash.[52] If the transaction was done by example cash the payment method would be done with something physical and therefor easier to trace, than virtual currencies that on the other end is something who is represented digital and does not have a physical appearance.

In later years, The use of virtual currencies was so important in the increase of digitalization that "virtual currencies" was defined and added in the AMLD 5, under article 3(1)(18)[53]*:" means a digital representation of value that is not issued or guaranteed by a central*

[50] Frame, W Scott, and Lawrence J White. *Technological Change, Financial Innovation, and Diffusion in Banking (*SSRN, 2014), 1-5.

[51] FATF report "Virtual Currencies Key Definitions and Potential AML/CFT Risks" Report, FATF, 2014, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk.html

[52] FATF report "Virtual Currencies Key Definitions and Potential AML/CFT Risks" pg. 9

[53] Directive 2018/843/EU art. 3(1)(18).

bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically". Also, the list of obliged entities was updated in the AMLD5 to include service providers of virtual assets.

1.9 Critical Legal Issues of the Current Regulatory AML-Framework

The different directives on anti-money laundering and combating the financing of terrorism, and the role of such as FATF and EBA is basis for the current AML-legislation. The framework and combating anti-money laundering are facing new challenges due to the new arisen era of technology and other new developments. This causes several limitations with the current legislation.

Firstly, the world is constantly increasing its technical perspective and the use of it. Such developments make it a necessity to have a legal framework within AML and CTF that can cope with rapidly changes. Further, the current legislation is shaped by different directives and therefor the different directives also needs to be transposition into each country national law.[54] For example, the different AML-directives needs to transposition into the Norwegian legislation. When the AML-directives are implemented into national law there can be delays because of the transposition. This can lead to a gap in the coordination between Financial Intelligence Units and national supervisors.[55] Other limitations in the current framework can be the need for application and harmonization of the legislation within the different EU countries.

[54] European commission, «Questions and Answers: Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT)" https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_3689
[55] European commission, «Commission steps up against money laundering and terrorist financing".

The legislation is changing: as mentioned by Minto, Andrea & Rasmussen, Niels. S, *Approaching the Danske Bank Scandal in a "Tragedy of the Commons" Perspective: Implications for Anti-Money Laundering Institutional Design and Regulatory Reforms in Europe*, in European Company and Financial Law Review, 2022, vol. 2, p. 306*"Governments and international organisations are calling for increased cooperation and regulation in contrasting money laundering practices. Once more and once again, EU financial regulation proves to a greater extent to be scandal-driven following the financial crisis and the publication of the seminal de Larosière report."*

Chapter II: Digital Onboarding

2.1 Introduction

This chapter approaches the topic of digital onboarding, and it is structured as follows: It starts with an introduction and then goes deeper into the current issues of digital onboarding. Then, a definition of digital onboarding is presented. The analysis moves to address the development of digital onboarding, followed by the future developments of the regulatory engagement with CDD and digital onboarding. Further, laws of digital onboarding are presented and examined, both hard laws and soft laws. In the end, the four activities of CDD are presented and hereunder the different risks of digital onboarding.

2.2 Definition of Digital Onboarding

Digital onboarding has arisen because of the increase of digital platforms in today's society, and this is leading to the digitalization of financial processes as well. Simply put, digital onboarding refers to how the customer enters into the relationship through digital portals and platforms. How the same expression tells, it indicates that the customer is enabled to start the relationship by means, or thanks to, a digital platform and that this customer relationship can be established from the comfort of their own home or wherever the customer is in the world. From a regulatory perspective, the development of digitalization and new ways to onboard, is forcing the supervisor and regulators to reevaluate and change the fundamental of financial law [56], because of the risks arising from the physical absence of the customer. This holds particularly true for the AML-legislation, given that its goal is to prevent money laundering, potential laundering of illegal funds and or that the illegal funds are used to finance terrorism. Also, the digital onboarding could lead to situation where it is difficult for the obliged to comply with the CDD-activities within the AML-legislation and this is opening up for the need for obliged entities to engage third parties to carry out the different CDD-activities[57], therefore opening up venues for strengthening the current legislation.[58]

[56] Frame, W Scott, and Lawrence J White. *Technological Change, Financial Innovation, and Diffusion in Banking (*SSRN, 2014), 1-5.
[57] EBA «Report on the use of digital platforms" (EBA/REP/2021/26), pg.15.
[58] Minto, Andrea""I'd love to help you, but I simply can't... or can I?" Anti-Money Laundering legislation and regulatory challenges concerning customer due diligence obligations in the platform era".

Further in a report on use of digital platforms amended by the European Banking Authority, a digital platform was defined as *"a technical infrastructure that enables at least one financial institution directly (or indirectly using a regulated or unregulated intermediary) to market to customers, and/or conclude with customers' contracts for financial products and services»*[59]. Meaning a way to obtain customers digitally, more specifically, digital onboarding is used digitally through platforms or portals to establish a financial relationship and is also used in the financial process. An example is when a customer of a bank wants to establish a customer relationship this can easily be done electronically and through the bank's website instead of needing to come by a bank office to become a customer.

2.3 Development of Digital Onboarding

The technological advancement and the use of digitalization in finance have made the European Union rethink and adapt along with the technological developments.[60] Indeed, technology developments are twofold. On the one hand, technology can be challenging, but on the other hand the same technology can also be a helpful tool for the different obliged entities and others that complies with the given AML/CTF-legislation.[61] The COVID-19 pandemic has both changed and is still changing the way customers and companies act within digital finance. The establishment of different business relationships and the ways of establishing such relationships had to be changed due to the lack of physical appearance during the pandemic. Companies needed to find ways and technical solutions to onboard customers digitally, but the companies also needed to make sure that the different AML and CTF legislation was complied with and obeyed. An example of this was the way to enter a new business relationship between a company and a customer. This is one of the main drivers of digital onboarding; the customer and the different represented companies could not meet face to face. This evolution can be seen see in today's business relationships. Now you can easily become a customer in a bank by only filling out a form digitally. After that, the bank needs to make sure that they are underlying all the legislation requirements, such as identification and ongoing monitoring of the established business relationship.[62] Further, the European Commission issued in September 2020 a digital

[59] EBA «Report on the use of digital platforms" (EBA/REP/2021/26), pg. 12.
[60] COM (2020) 591 final.
[61] FAFT "Opportunities and challenges of New Technologies for AML/CTF" Report, FATF, 2021, http://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf
[62] Directive 2015/849/EU art 13 (1).

finance strategy for the European Union and one of the priorities of the European Commission was to priority to remove the fragmentation in the digital single market.[63] In doing so the European Commission invited the European Banking Authority to contribute to the development of guidelines on the matter. As a result, the EBA provided several guidelines, and one of them was *the use of remote customer onboarding solutions under article 13 (1) of directive (EU) 2015/849*.[64]

2.3.1 The Future and Development of CDD and Digital Onboarding

CDD and digital onboarding may be changing. For instance, the regulation is changing its approach in the new proposal for a sixth AML directive, also referred to as AMLD 6.[65] Such as obliged entities outsourcing to other obliged entities, meaning passing out to someone who is considered a qualified entity. Further, Article 39 of the proposal allows obliged entities to rely on other entities to meet the CDD-requirements. This leading up to allowing outsourcing to someone who is not an obliged entity but an external service provider. Here there is chasing and elaborate on the approach, meaning that the legislation is denied changing view and liable obliged entities on the organizations says, and that obliged entities need to put in place both processes and procedures, such as safeguard in when delegation the task over to external service providers.[66] Such delegation of task over to external service providers will be elaborated and discussed further in the next and third chapter of this thesis.

2.4 Law on Digital Onboarding

The world's technological perspective is making the different financial institutions or others that go under the category of obliged entities, cf. article 2 of the fourth AML-directive[67] to think differently when obtaining or gaining a new customer. Today, you can more easily become a customer online and you do not have to physically go to an office to become a customer. This makes it more convenient to sign up as a new customer. Even so, such an easy way to become a customer is also raising concerns or challenges for the different financial

[63] COM (2020) 591 final.
[64] European banking authority. "Guidelines on the use of Remote Costumer Onboarding Solutions Under Article 13(1) of Directive (EU) 2015/849" (EBA/GL/2022/15).
[65] COM(2021) 423 final.
[66] European banking authority. "Guidelines on the use of Remote Costumer Onboarding Solutions Under Article 13(1) of Directive (EU) 2015/849" (EBA/GL/2022/15) pg. 22.
[67] Directive 2015/849/EU.

institutions that are underlying the compliance of CDD within the AML-legislation. There is soft law on digital onboarding, but these are not binding and are to be used as guidance on the matter. Therefore, both hard law and soft law will be presented in this part of the thesis. Starting with hard law and ending with the relevance of soft law.

2.4.1 Hard Law

CDD and digital onboarding is stipulated under article 13 in the fourth AML-directive, 2015/849. Article 13 directly says that obliged entities need to be implemented measures to comply with the customer's due diligence. To follow CDD of their customer the obliged entities need to follow the measures and the four activities in article 13, throughout the letters a-b. Further, the directive opens up in article 25[68] and also allows obliged entities to outsource to external service providers. The obliged entities still have the main responsibility even though CDD can be conducted by using third parties or so-called external service providers.

The earlier AML-directives had less technical perspectives and the newer AML-directives have evolved in the law-making process to follow along with the world's increasing technology. An example is the first AML-directive, Directive 1991/308/ECC.[69] Firstly, the only obliged entities were credit and financial institutions, and the only CDD was customer identification. The list of obliged entities changed in the later AML-directives because the criminals found new ways to launder money through other channels. It was not until the third AML-directive, Directive 2005/60/EC that the identification process went from only involving identification to also including due diligence.

Since the directive from 2015 and the paragraphs that regards the use of CDD and digital onboarding is laid down in a regulation, it makes that everything in the law will be the same in all regulations. This levelling also in outsourcing in paragraph 25 throughout paragraph 29 of the fourth AML-directive.[70]

The proposal for a sixth AML-directive is presenting important reforms of the current legal aml-framework. Is addressing the new technology instruments that allow criminals to launder money to finance terrorist activities with virtual currencies.[71]

[68] Directive 2015/849/EU art. 25-26.
[69] Directive 1991/308/EEC.
[70] Directive 2015/849/EU art. 25-29.
[71] FATF, "Updated Guidance for a Risk-Based Approach to Virtual Asset Service Providers".

2.4.2 The Relevance of Soft Law

Further, the world is increasing in the development of technology, this is leading up to digital onboarding of customer. As previously mentioned, during the COVID-19 pandemic, the European Commission (EC) requested EBA for assistance in developing soft laws such as guidance and recommendations on the matter of digital finance.[72] Nevertheless, the topic of CDD and digital onboarding is so important that the EBA issued some guidance on remote and digital onboarding.[73]

Also, an overall goal of the European Commission is by the year of 2024, to have harmonized and to have a more enacted AML and CTF framework for electronic solutions and the current and future digital era in financial services.[74] The priority also sets out for the development of a soft law funded by the EBA, because the European Commission asked the EBA for assistance in developing soft law such as guidance and recommendations on the matter of digital finance.

When it comes to digital onboarding and certain legislation on the matter there is also developed guidelines and recommendation. Since the different issued guidelines and recommendations are soft law this is also making the law not binding, this means that they do not have binding powers. For instance, European Banking Authority is using soft law through their guidelines and warnings. In particular, the FATF also gives out recommendations and guidance, and more recently an updated guidance on the riskiness of virtual currencies such as crypto.[75]

Soft laws are important in the law-making process and have been used to give documents such as guidance, recommendations, and reports. Soft laws can be developed when the current framework does not provide sufficient clarity on matters in the given legislation. To give an example, the report from the EBA about the use of remote customer onboarding solutions was developed to clarify the CDD rules in directive 2015/849. The aim was to highlight the focus on the digital and remote aspects and provide clarity on what was permitted and not permitted in the connection with digital and remote onboarding.[76]

[72] COM (2020) 591 final, pg.6.
[73] European banking authority. "Guidelines on the use of Remote Costumer Onboarding Solutions Under Article 13(1) of Directive (EU) 2015/849" (EBA/GL/2022/15) pg. 1.
[74] COM (2020) 591 final, pg. 5.
[75] FAFT, "Updated Guidance for a Risk-Based Approach to Virtual Asset Service Providers"
[76] EBA «Report on the use of digital platforms" (EBA/REP/2021/26), pg.12.

2.5 Risks of Digital Onboarding

To reduce risk in CDD, today and in the future, all the obliged entities need to have a good systems for identifying their customer, since most of the business relationships start online and on a digital platform.[77] Today CDD is composed of four activities that are indeed asking for certain cases of outsourcing. Different activities may bring the need for the obliged entities to ask for help and outsourcing of external service providers and onboarding because of the technical developments. Further, there are different risks in the matters of digital onboarding. The increasing digitalization is forcing regulators and supervisors to rethink basic financial laws.[78] Digital onboarding is making it easier to establish a business relationship at any time but is also raising some risk regarding the given AML-legislation. Besides, the new technology is also allowing new ways for criminals to launder illegal funds, and this is increasing the risk of money laundering and terrorist financing.

Firstly, there is the risk of the obliged entities and that they are not able to comply with article 13(1) of the Directive (EU) 2015/849 when using digital onboarding as a way to gain remote customer. Therefore, the CDD needs to be updated to new risks and ecosystems. A way of reducing the risk of digital onboarding is a risk-based approach. This means a general principal of AML-legislation that tells in substance that the recoverment should be designed and shaped for the riskiness of clients and the different companies.[79] Since, financial institutions, credit institutions and others are defined as obliged entities under article 2, this also means that they need to comply with the set AML-legislation. Therefore, the obliged entities need to comply with the different activities of CDD stipulated under article 13.

CDD is divided into different activities that need to be followed by the obliged entities. This can be a bridge to potentially suspicious transactions due to the difficult and complex process of following the activities that are set out in the AML-legislation. Obliged entities need to have an overall assessment of their clients, and outsourcing to external service providers may be necessary to obey the given AML-legislation. In the next chapter we will be going into details on outsourcing to external service providers.

[77] European Banking Authority "Report on the use of digital platforms. In the EU banking and payment sector" pg. 49-50.
[78] Frame, W Scott, and Lawrence J White. *Technological Change, Financial Innovation, and Diffusion in Banking (*SSRN, 2014), 1-5.
[79] FATF "Guidance for a risk-based approach. The banking sector".

2.5.1 Identifying the Customer

Identification of the customer is established under article 13(1) letter a:[80] *"identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source"*. The identification of the customer is the process where the information and authenticity of the customer are being processed, and such collected material can verify the customer's identity.

A risk with identifying the customer is that the obliged entity does not verge upon that the customer is impersonating someone else. In the EBA *Guidelines about the use of remote customer onboarding solution*, the EBA highlights the importance of the quality of data, video, images of the customer need to be doubtless to recognize.[81] If such materials are not collected during the onboarding the obliged entities may end up breaching the AML-legislation. This can be by not being able to reveal the customer who is an impersonator or needing to put in extra measures to uncover this. Also, such a scenario will make it difficult for the obliged entities to verify a certain customer in case of a suspicious transaction.

Further, another risk is that the information that are obtained through digital onboarding are not up to date.[82] Such outdated information on a customer can lead to breach in the legislation if the information that was obtained when establishing the customer relationship is no longer adequate or correct. This can for example be if the collected image to identify the customer was taken long ago and this makes the customer not clearly recognizable.

2.5.2 Identifying the Beneficial Owner

The identification of the beneficial owner within AML is established under article 13(1) letter b[83]: "*identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure*

[80] Directive 2015/849/EU art. 13 (1) (a).
[81] European banking authority. "Guidelines on the use of Remote Costumer Onboarding Solutions Under Article 13(1) of Directive (EU) 2015/849" (EBA/GL/2022/15) pg. 16.
[82] European banking authority. "Guidelines on the use of Remote Costumer Onboarding Solutions Under Article 13(1) of Directive (EU) 2015/849" (EBA/GL/2022/15) pg. 16 point 24 a).
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1019865/EBA%20Digital%20platforms%20report%20-%20210921.pdf
[83] Directive 2015/849/EU art 13 (1) (b).

of the customer». The identification of the beneficial owner is the process where the rightful owner of a transaction is being checked and finding out if the owner of the transaction is whom they seem to be.

A risk in identifying the beneficial owner is that remote onboarding can make it challenging to identify the beneficial owner. For example, if the information that was collected when the customer relationship was vague, outdated or wrongfully given this can make it hard for the obliged entity to identify the beneficial owner. Therefore, the financial institution that use digital onboarding needs to have implemented good systems to verify the different customer, so they comply with CDD in AML-legislation.[84]

2.5.3 Obtaining Information About Customers

The obliged entities are required to obtain information about their customer, and this is set out in letter c of article 13(1) as:[85] *"assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship."* Meaning that obliged entities are responsible of collecting information about their customer. When obliged entities obtaining information about customer, they can detect a breach of the AML-legislation, such breach can be suspicious and maybe illegal transaction made by their customer. For an example, in a bank, a risk with obtaining information about customer can be that the obliged entity does not obtain additional information or enough information about their customer.[86] Weakly or missing information on a customer can be a risk since this can make it harder for the obliged entity to verify information.

2.5.4 Ongoing Monitoring of the Business Relationship

Lastly, the business relationship between the obliged entity and a customer does not end once the relationship is established. This established under article 13(1) letter d as: [87]*"conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the*

[84] Guidance, FAFT "Guidance on Beneficial Ownership for Legal Person" pg. 6-7 https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-Beneficial-Ownership-Legal-Persons.html
[85] Directive 2015/849/EU art 13 (1) (c).
[86] Guidance, FATF " Guidance for a risk-based approach. The banking sector"pg.19.
[87] Directive 2015/849/EU art 13 (1) (d).

customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date» Therefore, in order to comply with the different AML-legislations and the fourth activity of CDD, the obliged entities need to keep monitoring their customer. A report from the EBA *on the use of digital platforms*[88] also sets out some AML and CTF risk when it comes to digital onboarding. For instance, the obtaining information, ongoing monitoring of a customer and the use of KYC can be a risk because of the different way of approaches from the different authorities.[89] In today's AML-legislation there is no single rulebook when it comes to the AML-legislation and the different AML-directives, but this is one of the priorities in the proposal for an upcoming aml directive (AMLD 6).[90]

Furthermore, another risk can be the different approach from the unsimilar third parties such as external services providers that does the CDD process on behalf of the obliged entities. The obliged entities sometimes need to ask for support to comply with the different digital solutions, and this is when the external service providers come in. In the next chapter we will be entering into detail about outsourcing to external services providers.

[88] European Banking Authority "Report on the use of digital platforms. In the EU banking and payment sector" (EBA/REP/2021/26).
[89] European Banking Authority "Report on the use of digital platforms. In the EU banking and payment sector" (EBA/REP/2021/26), pg. 49.
[90] COM (2021) 420 final "1. Context of the proposal".

Chapter III: Outsourcing to External Service Providers

3.1 Introduction

In the final chapter of the thesis the different aspects related to outsourcing of customer due diligence activities to external service providers are examined. First, a definition of outsourcing to external service providers is presented, hereunder both a definition that focuses on the financial sector and also a definition on outsourcing given by the EBA. Following, are an introduction to different soft law and hard law on the topic. Then the thesis goes deeper into the different hard law and development of soft law on outsourcing of CDD-activities. Thereafter, the new proposed anti-money laundering regulations with a focus on outsourcing to third parties are examined, followed by the risks related to outsourcing. Lastly, the chapter also discuss liability and both advantages and disadvantages when it comes to outsourcing the different CDD-activities to external service providers.

3.2 Definition on Outsourcing to External Service Providers

As demonstrated in previous chapters CDD is formed by four different activities: [91]*1) Identifying the customer; 2) identifying the beneficial owner; 3) obtaining information; and 4) conducting ongoing monitoring of the business relationship.* Over time and new complicity by digitalization it may be complicated to conduct and carry out such activities.

The increase of digitalization and solutions such as digital onboarding can result in making the required activities of CDD more difficult to comply with for the different obliged parties. This has led to the obliged entities needing to ask for support to comply with the digital solution and this is when the use of outsourcing external service providers come in. Making the obliged entities outsource to external service providers that can give support to help with their obligations.

In the financial sector the concept of outsourcing has been known since around the 2000.[92] However, the use and development of outsourcing has changed due to the increase of new technology and ways to outsource. Even tough outsourcing is a wide conception, a given definition on outsourcing in the financial sector is: *"The use of a third party for the performance of any aspect of the outsourcing firm`s material functions that would otherwise be undertaken*

[91] Directive 2015/849/EU art. 13 (1) a-d.
[92] Peter Laaper, *European Financial Regulation* (Oxford: Hart Publishing, 2021), 255.

by the entity itself".[93] Also, the EBA issued guidelines on outsourcing in 2019 and defined outsourcing to "*means an arrangement of any form between an institution, a payment institution or an electronic money institution and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the institution, the payment institution or the electronic money institution itself.*".[94] The definition given by the EBA can be applied to our case when it comes to outsourcing to external service providers. Since we do not have a specific definition in the AML-legislation we have to look somewhere else to get a definition. It is odd that in a special regulation on AML a specific definition on outsourcing is not provided, but maybe such a clear and specific definition will be given in the future.

3.3 Law on Outsourcing to External Service Providers

Outsourcing of CDD activities has become a more and more common practice in the context of AML and CTF regulations. The use of external service providers is subject to soft and hard laws. However, these may vary depending on the jurisdiction. Especially within the EU in lately relationship hard law and soft law are very fascinating and a hard relationship. On one hand, there are soft laws such as guidelines issued by regulatory bodies which provides non-binding recommendations for practices of outsourcing to external service providers. Soft law is providing guidance and such documents that are issued by EBA and FATF are important. It allows the legislator to be up to date to marked practice and when legislator use such guidance for hard law, this show that such soft law is in line with the need to follow the transformation of the marked and always emerging practices. On the other hand, there are hard laws such as legislations which impose mandatory obligations for obliged entities such as financial institutions. Therefore, the different financial institutions must in line with the legislations, manage the risks associated with outsourcing CDD any comply with AML and CTF regulations.

[93] Peter Laaper, *European Financial Regulation* (Oxford: Hart Publishing, 2021), 255.
[94] European Banking Authority "Final report on EBA Guidelines on outsourcing arrangements" (EBA/GL/2019/02) pg.19 nr.12.

3.3.1 Hard Law

As mentioned earlier in this chapter, outsourcing to third parties such as external service providers are provided by the obliged. This is because of the many task and obligations that the different obliged entities need to comply with to fulfill the CDD obligation in the AML-legislation. Directive 2015/849 (EU) provides opportunities for third parties to perform customer due diligence tasks on behalf of obliged entities. Section IV and articles 25-29 outline the possibility of outsourcing certain CDD task to third parties.[95] This enables obliged entities to delegate task such as identifying the beneficial owner to third parties.[96]

Firstly, in the IV section, is article 25. In this paragraph the use of third parties, hereunder external services providers are presented:[97] *"Member States may permit obliged entities to rely on third parties to meet the customer due diligence requirements laid down in points (a), (b) and (c) of the first subparagraph of Article 13(1)"*. Meaning that the legislation opens up for the obliged entities relying and outsourcing to a third party. However, the last part of article 25 states that the ultimate responsibility for the compliments and requirements of article 13 (1) a-b rests on the obliged entities.

Moreover, a definition of "third parties" is provided under article 26 of the directive and states that: [98] *"obliged entities listed in Article 2, the member organisations or federations of those obliged entities, or other institutions or persons situated in a Member State or third country that..»*. The article sets off requirements that the third parties need to follow. This is to be found under letter a) of the article and it stipulates that the third parties need to "*apply due customer diligence and record-keeping requirements that are consistent with those laid down in the directive"*, cf. article 26(1) letter a. A second condition is under the letter b) and states the need to "*have their compliance with the requirements of this Directive supervised in a manner consistent with section 2 of chapter IV"*, cf. article 26 (1) letter b. This article opens up for outsourcing to other parties. However, one potential issue with article 26 is that it can limit the ability to outsource different CDD activities and obligations to only obliged entities. This leads to potentially exuding out other external service providers. This potential issues with outsourcing will be revisited later on in this chapter.

[95] Directive 2015/849/EU art. 25-29.
[96] Directive 2015/849/EU art. 13 (1) a-d.
[97] Directive 2015/849/EU art. 25 (1).
[98] Directive 2015/849/EU art 26(1).

Despite that article 26 only allows outsourcing to other qualified parties, there can be a found an exception for section IV in article 29. The article stipulates that: [99]*«This Section shall not apply to outsourcing or agency relationships where, on the basis of a contractual arrangement, the outsourcing service provider or agent is to be regarded as part of the obliged entity»*.

Additionally, the responsibility of the member states is laid down in article 27, saying that: [100]"*Member States shall ensure that obliged entities obtain from the third party relied upon the necessary information concerning the customer due diligence requirements laid down in points (a), (b) and (c) of the first subparagraph of Article 13(1)*» This means that the responsibility of members states are to ensure that the obliged entities, such as banks and financial institutions [101], receive the required information from the outsourcing third parties to properly conduct CDD requirements. Further, article 27(1) takes on the responsibility of the member states to ensure that the obliged entities receive relevant copies when requesting this from the third-party providers. Such relevant copies can be copies of identification and verification data of the customer.[102]

The regulation of rules concerning outsourcing are scattered, so it is not really clear what we can do. One side straight where you only can outsource to obliged entities under article 2 of AMLD 4.[103] Since it is a directive it has been implemented by all jurisdiction, but we have different national law, and it may arise some differences when interoperated into national law. The given directive is telling the member states what to do, but again since we are talking about directive there are a problem with implementing into national law. Throughout, article 25-26 with the discretion that member states have in dissuading the rules, but this can cause uncertainty when we talk about AML. This problem is even more serious if we think it directly allows the member states to have different change depending on the jurisdiction.

[99] Directive 2015/849/ EU art 29.
[100] Directive 2015/849/EU art. 27(1).
[101] Directive 2015/849/EU art. 2.
[102] Directive 2015/849/EU art 27(2).
[103] Directive 2015/849/EU art. 2.

3.3.2 Development of Soft Law

The development of outsourcing is constantly changing intact with the world, and this leads to the need of relevant guidelines and framework.[104] Soft law has been a part in creating frameworks that adapt to the evolving of the world.

FATF promotes effective implementation of legal and regulatory, and operational measures for combating money laundering, terrorist financing, and other related threats to the integrity of financial institutions. They have been on the front of the development in regard of recommendations. Also, they have provided recommendations on how countries should approach customer due diligence, including when outsourcing such services to third-party service providers.[105]

As previously mentioned in the thesis, the EBA have issued some guidelines on digital onboarding because of the importance of the topic. The EBA has done the same with outsourcing and issued several guidelines on the topic. This is to ensure that banks and other financial institutions act appropriately and effectively in managing the risks associated with outsourcing CDD activities.

Today, there are more soft laws then hard laws when it comes to the topic of outsourcing. Soft laws regarding outsourcing is also important when it potentially can lead to hard laws. This has led to the newest guidelines on outsourcing from the EBA. In the *final report on EBA Guidelines on outsourcing arrangements* EBA focus on outsourcing and provide directions for the institutions that use outsourcing, this can example be payment institutions and electronic money institutions. The guidelines focus on outsourcing on important or critical functions and emphasize the importance of risk management in these cases.[106] The purpose of the guidelines is to ensure that outsourcing providers has adequate skills, knowledge, resources to perform CDD activities, has sufficient instructions on how to deal with CDD activities, and complies with legal and regulatory requirements. Institutions have a responsibility to monitor and oversight procedures to ensure that the outsourcing arrangement meet the requirements, however, this is no explicitly forceable. This may change as of the upcoming reform of the EU AML Regime which will be explained later in this chapter.

[104] European Banking Authority "Final report on EBA Guidelines on outsourcing arrangements" (EBA/GL/2019/02) pg.7.
[105] FATF Recommendations ""International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation" Pg.18 nr.17.
[106] European Banking Authority "Final report on EBA Guidelines on outsourcing arrangements" (EBA/GL/2019/02) pg pg.7 nr.5.

This shows that there are a couple of places for organizations to find recommendations on how they should proceed when wanting to outsource CDD activities to external service providers. However, it is important to emphasize that these are only recommendations and guidance and not binding laws. However, as mentioned earlier in this subchapter, soft laws can provide important guidance to legislator. This came to show when the European Commission asked the EBA to issue *guidelines on the use of Remote Customer Onboarding Solutions*.[107]

3.3.3 Upcoming Reform of the EU AML Regime

The upcoming reform of the EU Anti-Money Laundering regime is changing everything with new authority (AMLA) and a new AML- regulation within EU.

The aim is to strengthen EU´s legal framework for preventing money laundering and terrorist financing.[108] The upcoming reform is proposing a completed constitution and setting of AML regulatory framework. The proposal suggests several changes to address weaknesses in the current AML regime. The upcoming reform wants to expand the scope of the AML regulations to cover all virtual currencies, establish a centralized public register of beneficial ownership information for companies operating in EU, introduce additional due diligence requirements for obliged entities (such as enhanced CDD measures for high-risk transactions), and increase powers and resources of EU AML regulators to ensure better oversight and enforcement of the AML regulations.[109] Talking about the possibility to outsource relating to CDD and an increase in details of rules and sure that every country will have the same rules and obliged entities have same opportunity, to use the support of external service provider.[110]

The commission presented in 2020: proposal COM (2021) 420 final, *proposal for a regulation of the European parliament and of the council on the prevention of the use of*

[107] "Guidelines on the use of Remote Costumer Onboarding Solutions Under Article 13(1) of Directive (EU) 2015/849" (EBA/GL/2022/15).

[108] News European Parliament, "New EU measures against money laundering and terrorist financing", *European Parliament.https://www.europarl.europa.eu/news/en/press-room/20230327IPR78511/new-eu-measures-against-money-laundering-and-terrorist-financing*

[109]COM(2021) 423 final.

[110] COM (2021) 421 final, under 1.Context of the proposal**.**

financial system for the purpose of money laundering or terrorist financing.[111] As mentioned earlier in the thesis, European Commission presented 6 different priorities:[112]

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

2. Establishing an EU single rulebook on AML/CFT,

3. Bringing about 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.

Chapter 6 of the proposal of regulation go into the performance of third parties. throughout article 38 till 44. Article 39 allows obliged entities to rely on other entities to meet the CDD-requirements. This means that the regulation opens up for other than obliged entities to outsource. The regulation is acknowledgment the possibility for obliged entities to use service providers that are not necessarily obliged entities. As showed in previous part is that an obliged entity, for example a bank can only rely on obliged entities to conduct the different CDD activities. However, the proposal on the new regulation is proposing that there is a possibility to allow external service providers to conduct activities within CDD. Such, a wider set of choices that obliged entities can make when they want to give CDD to others can open up for technology help. For example, technology help can be the use of AI and biometrics.[113] This can be support from an external service provider on facial recognition to identify the customer in a digital onboarding process. Digital onboarding as earlier mentioned in this thesis are not separated but are also put in the context with outsourcing.

[111] COM (2021) 420 final.

[112]Com (2021) 420 final "1. Context of the proposal".
[113] European Banking Authority " Final report on Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849" (EBA/GL/2021/02) pg. 44 https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/revised-guidelines-on-ml-tf-risk-factors

Further, outsourcing is presented in article 40 and states that: [114]"*Obliged entities may outsource tasks deriving from requirements under this Regulation for the purpose of performing customer due diligence to an agent or external service provider, whether a natural or legal person."* Meaning that obliged entities may outsource to external service providers to comply with the given CDD-requirements. Despite this, there is an exception in article 40(1) when it comes to natural or legal person who is a resident or have an establishment in a third country.

Lastly, in article 41 the proposal gives some guidelines on the performance by third parties:[115] *«a) the conditions which are acceptable for obliged entities to rely on information collected by another obliged entity, including in case of remote customer due diligence; (b) the establishment of outsourcing relationships in accordance with Article 40, their governance and procedures for monitoring the implementation of functions by the outsourced entities, and in particular those functions that are to be regarded as critical;(c) the roles and responsibility of each actor, whether in a situation of reliance on another obliged entity or of outsourcing; (d) supervisory approaches to reliance on other obliged entities and outsourcing*». Meaning that these guidelines can intend to promote transparency and accountability of obligated entities such as financial institutions. They are supposed to ensure best practices in regard of outsourcing customer due diligence activities to external service providers. Transparency and accountability are vital as such services are sensitive and critical. Further, third parties are qualified parties and are therefore obliged entities, therefore there is very important with regulation on a wider set of actors that also can be justified by the new challenges by the increase of digitalization.

After this proposal another proposal was published by the European Commission: A regulation, In the COM (2021) 423 final a proposal for a directive which eventually can replace the current AML-directive, directive 2015/849/EU.[116]

[114] COM (2021) 420 final. Art. 40.

[115] COM (2021) 420 final, Art. 41.
[116] COM (2021) 423 final.

3.4 Risks of Outsourcing

There are different risks when it comes to outsourcing to external service providers. Such risks could be related to data security and confidentiality, compliance (in regard of legal and regulatory requirements), quality control, communication and coordination, and cost and resources[117]. Obliged entities, such as financial institutions have a responsibility to ensure that the requirements are meet, however this can be difficult when CDD activities find place outside of the institutions.

When it comes to hard law on the topic, article 13 of AMLD4 says something about the risk of CDD and measures that need to be established by the obliged entities: [118] "*obliged entities may determine the extent of such measures on a risk-sensitive basis. Member States shall require that obliged entities take into account at least the variables set out* in Annex *I when assessing the risks of money laundering and terrorist financing"*. However, obliged entities may have different interpretations of the level of risk associated with a particular situation. Thus, the hard law relies on the subjective assessment of the obliged entity. Also, the organizational measures can be differently depending on the risk assessment done by each of the obliged entities.

With the Directive 2015/849/ (EU) new concerns arise, these must be carefully explored. For example, the directive can be interpreted as the regime provides exclusive rights to parties which are qualified and subjected to the AML legislation. However, who are these so-called qualified parties? Sharing the concern of Minto[119], there are numerous of providers, and these do not necessarily fall within the notion "third parties". This is because they are not labelled as "obliged entities". This highlight the unclarity regarding outsourcing CDD activities to external service providers. Earlier in accordance with AML-directives, obligated entities only included credit and financial institutions. However, later obliged entities have expanded to providers of gambling services, and newly service providers of virtual currency.[120] This is due to the increasing technology in the world and new ways of laundering money from activities which are criminal or financing terrorism.

[117] European Banking Authority "Final report on EBA Guidelines on outsourcing arrangements" (EBA/GL/2019/02).
[118] Directive 2015/849/EU art. 13 (2)(3).
[119] Minto, Andrea""I'd love to help you, but I simply can't... or can I?" Anti-Money Laundering legislation and regulatory challenges concerning customer due diligence obligations in the platform era".

[120] Directive 2018/843/EU art.3 (1) (18).

When it comes to soft law, EBA in their report on "Final report on EBA guidelines on outsourcing arrangements says that the institutions and payments institutions shall ensure that:[121] *"the risks related to current and planned outsourcing arrangements are adequately identified, assessed, managed and mitigated, including risks related to ICT and financial technology (fintech)»*. Meaning that the institutions that outsource have a potential risk with adequality identifying, and any risk related to information and communication technology (ICT) as well as financial technology (fintech). If the obliged entities do not put in sufficient measures to manage such risks, this can lead to negative consequences of the CDD activities that are outsourced. For example, this can lead to that art. 13 (1) (a) with identifying the customer is not up-to-date, and this can make it hard to identify the customer that have a relationship with the financial institution such as a bank, and therefore the bank may need to ask the customer to send in up-to-date identification.

Furthermore, EBA address risks related to outsourcing in their recommendations. For instance, in a *final report regarding CDD and the factor credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationship and occasional transactions*[122]. In this report there are pointed out some risk factors that the different financial and credit institutions need to take into consideration. Some risks that the EBA points out is:[123] "*a) the extent to which the business relationship is conducted on a non-face-to-face basis; and b) any introducers or intermediaries the firm might use and the nature of their relationship with the firm. »* This is risks that the obliged entities should include when they are putting in *measures on a risk-sensitive basis*, cf. 13 (2)(3) in AMLD 4. Further, there are some factors that should be considered when it comes to risks. This is stipulated as:[124] "*When assessing the risk associated with the way in which the customer obtains the products or services, firms should consider a number of factors:"* Further, such factors may be:[125] "*whether the customer has been introduced by a third party"* or "*to the extent permitted by national legislation, when the firm uses an outsourced service provider for aspects of its AML/CFT obligations, whether it has considered whether the outsourced service provider is an obliged entity"*.

[121] European Banking Authority "Final report on EBA Guidelines on outsourcing arrangements" (EBA/GL/2019/02)pg. 34 point 40 (c).
[122] European Banking Authority " Final report on Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849" (EBA/GL/2021/02).
[123] EBA/GL/2021/02 pg. 35 point 2.20 (a).
[124] EBA/GL/2021/02 pg. 35 point 2.21 (c) (f).
[125] EBA/GL/2021/02 pg. 35 point 2.21.

Finally, the obliged entitles should be open about their use of external service providers and the fact that they refrain from developing in-house innovative solution to avoid any confusion regarding the responsible party for conducting various CDD-activities. This is also stipulated by the EBA in their final report on ML and CT Risk factors.[126]

3.4.1 Liability

Even tough, the obliged entities outsource to external services providers, the main responsibility when it comes obtaining the AML-legislation is still different when it comes to liability for the obliged entities and the third parties. Also, article 25 of the AMLD 4 states that the *"the ultimate responsibility for meeting those requirements shall remain with the obliged entity which relies on the third party"*.[127] So, at the end of the day the responsibility when it comes to outsourcing is laid down on the obliged entities. Therefore, it is important that the activities of CDD and that the overall AML-legislation is to be followed and obeyed with by the party that is conducting the outsourcing.

Further, it is important that there have been implemented safety measures and that the obliged entities such as financial institutions have followed the risk assessment after article 13 in AMLD 4.[128] The obliged entities therefore need to ensure that the service provider is both capable and qualified of performing the required CDD tasks and in compliance with the all the relevant regulations. If this is not fully ensured, the obliged entities may risk a breach in the legislation, and this making the obliged entities fully liable for the breach.

Since the obliged entities have the ultimate responsibility, this also means in cases for data security and privacy. Therefore, the obliged entities need to make sure that the service provider have carried out both technical and organizational measures when protecting the data of the customers.[129] Meaning that the obliged entities need to make sure that their customers data is handled both correct and appropriate by the external service provider. A risk here can for example be if the external service providers does not have implemented measures for data security and privacy. Such breaches can lead to leaks in collected data of the customer like their identification (passport, id-card, picture), audio, video and more. In such's scenarios the obliged entity may become liable for the breach even though it is done by the external service providers.

[126] EBA/GL/2021/02 pg. 44 point 4.34.
[127] Directive 2015/849/EU art. 25 (2).
[128] Directive 2015/849/EU art. 13 (2)(3).
[129] European Banking Authority "Final report on EBA Guidelines on outsourcing arrangements" (EBA/GL/2019/02) pg. 43.

Conclusion

The rise of digital alternatives such as decrease in face-to face interaction between financial institutions and their customers has raised challenges concerning the customer due diligence (CDD) in the anti-money laundering legislation (AML). Although this development makes it harder to monitor and detect money laundering and terrorist financing activities, and it can also provide new opportunities for criminals to launder money. Nonetheless, the advancement in technology have also simplified the financial process. With allowing onboarding and also outsourcing of different CDD activities. An example of easier process is in the banking process, allowing customer to register with a bank using their tablets, computers or even their phone from the comfort of their homes.

The current state of the customer due diligence (CDD) within anti-money laundering legislation (AML) illustrates that as a directive, the different AMLD have been adopted by all jurisdictions. The development of AML directives show that regulations obliged entities are subject to, are becoming more and more complicated. This has both upsides and downsides, requiring more resources and effort from obliged entities, while also make it easier prevent money laundering. Moreover, differences in national law may arise when interpreting and implementing the directive in each county's legal system. This can potentially cause a gap between different legislation within the European Union. Hence, it may be more difficult to achieve the attended goals of the directive and create confusion and uncertainty for business operating internationally.

The analysis of digital onboarding in customer due diligence (CDD) in Anti-Money Laundering (AML) legislation highlights the growing trend of businesses acquiring customer through digital platforms. The use of onboarding gives advantages such as easier access to onboarding customers digitally and an efficient process for the financial institutions and their customers. However, some disadvantages of this is the challenges for financial institutions to accurately identify their customer, leading to a need of increased resources and investigation effort in obtaining information and to be able to perform the different CDD activities under article 13 of AMLD 4. As a result, organizations subjected to AML legislation are seeking alternative method to fulfill their obligations, which has led many obliged entities to outsource the responsibilities of CDD activities to other service providers.

Further, the analysis of outsourcing to external service providers for CDD requirements in AML legislation revealed a lack of clarity regarding which entities were qualified parties to offer the services of outsourcing. There are benefits of outsourcing, it requires less resources

and work in-house. However, it also causes some concerns. Even though the obliged entities outsource, they still have the liability in regard of requirements. Thus, while outsourcing, the obliged entities must have a certain control over the external provider to ensure that CDD activities are being complied and uphold. They also need to implement and conduct CDD measures to the required standard within the external provider. Outsourcing can lead to new risks for the obliged entities, such as data security risks or not having updated identification on their customers. Having some control and having measures within in the external provider is therefore important. Moreover, the analysis indicates that who these external service providers are, is unclear as there are different definitions and exceptions. Hence, there is still some improvement regarding outsourcing in the AML regulations.

Soft laws such as guidelines were not clear on the matter of outsourcing to external service providers, but newer legal sources such as the proposal for the new AMLD 6, COM (2021) 423 final can provide more specificity. Such vagueness may be due to process of developing AML-legislation intact with the arise of new technology and other new areas of expanding. Lastly, as the directives has expanded and developed, the focus when it comes to outsourcing of CDD-activities has shifted from who is the most eligible to perform these activities to how they should be carried out by external parties.

In conclusion, the thesis highlights the challenges of new expanding areas when it comes to the customer due diligence (CDD) in the Anti-Money laundering legislation (AML). Also, the thesis emphasises that the obliged entities have more responsibility than ever to prevent money laundering and combat criminality. The analysis reveals a shift from focusing on who can provide outsourcing services for CDD-activities to how these outsourcing services should be facilitated by the obliged entities for maximum benefit.

List of Sources

Books and articles

Arner, Douglas W, Dirk A Zetzsche, Ross P Buckley, and Janos N Barberis. "The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital Kyc Utilities." *European business organization law review* 20 (2019): 55-80.

Colaert, Veerle, Danny Busch, and Thomas Incalza. *European Financial Regulation: Levelling the Cross-Sectoral Playing Field.* Oxford: Hart Publishing, 2021.

Cox, Dennis. *Handbook of Anti Money Laundering*. 1. ed. Chichester, England: Wiley, 2014

Frame, W Scott, and Lawrence J White. *Technological Change, Financial Innovation, and Diffusion in Banking.* SSRN, 2014.

Gál, István László. "The 2018/843 EU Directive on the Prevention of Money Laundering and Terrorist Financing and Its Correlation to the Criminal Law Prevention of the Stock Markets." (2019). http://real.mtak.hu/100887/1/The2018-843EUDirectiveonthePreventionofMoneyLaundering.pdf.

Gottschalk, Petter, and Ove Olsen. *Økonomisk Kriminalitet: Ledelse Og Samfunnsansvar*. Oslo: Cappelen Damm Akademisk, 2016.

Sharman, J. C. *The Money Laundry: Regulating Criminal Finance in the Global Economy*. Cornell Studies in Political Economy. Ithaca N.Y.: Cornell University Press, 2011.

Minto, Andrea "I'd love to help you, but I simply can't... or can I?". Anti-Money Laundering legislation and regulatory challenges concerning customer due diligence obligations in the platform era". *Europäische Zeitschrift für Wirtschaftsrecht.* ISSN 0937-7204 s.986-993,(2022)

Minto, Andrea and Skovmand Rasmussen, Niels. "Approaching the Danske Bank Scandal in a "Tragedy of the Commons" Perspective: Implications for Anti-Money Laundering Institutional Design and Regulatory Reforms in Europe" *European Company and Financial Law Review* 19, no. 2 (2022): 305-338. https://doi.org/10.1515/ecfr-2022-0010

Mitsilegas, Valsamis, and Bill Gilmore. "The Eu Legislative Framework against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards." *ICLQ* 56, no. 1 (2007): 119-40. https://doi.org/10.1093/iclq/lei152.

Rui, Jon Petter, and Norge. *Hvitvasking : Fenomenet, Regelverket, Nye Strategier*. Oslo: Universitetsforlaget, 2012.

Siclari, Domenico. *The New Anti-money Laundering Law: First perspectives on the 4th European Union Directive*. Cham: Springer international publishing, 2016.

Wilson, John O. S ; Berger, Allen N ; Molyneux, Philip. *The Oxford Handbook of Banking*. Oxford: Oxford University Press, Incorporated, 2010.

Council of Europe

Guidance, FATF "Guidance for a risk-based approach. The banking sector" edited by FATF Guidance, October 2014. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Risk-based-approach-banking-sector.html.

Report, The FATF "Virtual Currencies Key Definitions and Potential AML/CFT Risks" edited by the FATF, June 2014, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk.html.

Recommendations, the FAFT "Terrorist Financing Risk Assessment Guidance" edited by the FATF Recommendations, 2019. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Terrorist-financing-risk-assessment-guidance.html.

The FATF recommendations "Consolidated Processes and Procedures for Mutual Evaluations and Follow-Up "Universal Procedures" edited by the FATS, Recommendations, September 2019. https://www.fatf-gafi.org/en/publications/Fatfgeneral/Universal-procedures.html

FATF "Opportunities and challenges of New Technologies for AML/CTF" FAFT, Paris, France,2021. http://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf

FATF, "Updated Guidance for a Risk-Based Approach to Virtual Asset Service Providers", FATF, Paris, 2021. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

Recommendations, The FATF. "International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation of Weapons of Mass Destruction" edited by The FAFT Recommendations, 2022. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

Guidance, FATF "Guidance on Beneficial Ownership for Legal Person" edited by the FATF, March, 2023. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Beneficial-Ownership-Legal-Persons.pdf.coredownload.pdf

Recommendations, the FATF (2012-2023) "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation" edited by the FATF recommendations, 2023. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

FAFT, "What We Do." 2023. Retrieved: 08.02, 2023, https://www.fatf-gafi.org/en/the-fatf/what-we-do.html.

European Union

Council Directive 91/308/EEC *of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering*.

Directive 2001/97/EC *of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering.*

Directive 2005/60/EC *of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.*

Commission Directive 2006/70/EC *of 1 August 2006 laying down implementing measures of Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of politically exposed person and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis.*

Directive (EU) 2015/849 *of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, 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.*

Directive (EU) 2018/843 *of the European Parliament and of the Council 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.*

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 and relating to cross-border activities” (SWD/2019/650 final)

European Commission “report from the commission to the European Parliament and the Council assessing the framework for cooperation between Financial Intelligence Units” (COM/2019/371 final)

European Commission “Report from the Commission to the European Parliament and the Council on the interconnection of national centralized automated mechanisms (central registers or central electronic data retrieval systems) of the Member States on bank accounts” (COM/2019/372 final)

European Commission, “Report from the Commission to the European Parliament and the Council on the assessment of recent alleged money launder cases involving EU credit institutions” (COM/2019/373 final)

European Commission. “Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions on a Digital Finance Strategy for the EU” COM (2020) 591 final

European Commission, "Questions and Answers: Anti-Money Laundering and Countering Financing of Terrorism (AML/CTF)." 2021, accessed 02.02, 2023, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_3689.

Final Report, European banking authority. “Guidelines on the use of Remote Costumer Onboarding Solutions Under Article 13(1) of Directive (EU) 2015/849” (EBA/GL/2022/15)

European Banking Authority “Final report on EBA Guidelines on outsourcing arrangements” (EBA/GL/2019/02)

European Banking Authority “Final report on Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (‘The ML/TF Risk Factors Guidelines’) under Articles 17 and 18(4) of Directive (EU) 2015/849” (EBA/GL/2021/02)

News European Parliament, “New EU measures against money laundering and terrorist financing”, *European Parliament.* Accessed 11.05.23. https://www.europarl.europa.eu/news/en/press-room/20230327IPR78511/new-eu-measures-against-money-laundering-and-terrorist-financing

Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States 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 (COM/2021/423 final)

Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast) (COM/2021/422 final).

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 (COM/2021/420 final).

Norwegian Legislation

Lov av 6. januar 2018 nr. 23 om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven) (Law 6. January 2018 no.23 Act relating to Measures to Combat Money Laundering and Terrorist Financing (the Anti-Money Laundering act) https://lovdata.no/pro/#document/NLE/lov/2018-06-01-23

Lov av 20. mai 2005 nr. 28 om straff (straffeloven) (Law 20. May 2005 no. 28 The penal code) https://lovdata.no/pro/#document/NLE/lov/2005-05-20-28

FOR-2018-09-14-1324 Forskrift om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsforskriften)

Prop. 40 L (2017-2018). *Lov om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven).* Oslo: Finansdepartementet. https://www.regjeringen.no/no/dokumenter/prop.-40-l-20172018/id2589604/

Prop.92 LS (2019–2020) Lov om finansavtaler (finansavtaleloven) og samtykke til godkjennelse av EØS-komiteens beslutninger nr. 125/2019 og 130/2019 av 8. mai 2019 om innlemmelse i EØS-avtalen av direktiv 2014/17/EU om kredittavtaler for forbrukere i forbindelse med fast eiendom til boligformål (boliglåndirektivet) og delegert kommisjonsforordning (EU) nr. 1125/2014.mv Oslo: Finansdepartementet. https://www.regjeringen.no/no/dokumenter/prop.-92-ls-20192020/id2700119/

Websites

FATF official website: www.fatf-gafi.org

Finanstilsynet, "Hvitvaskingsregelverket Og Krav Til Gyldig Legitimasjon.", 2022 https://www.finanstilsynet.no/tema/hvitvasking-og-terrorfinansiering/hvitvaskingsregelverket-og-krav-til-gyldig-legitimasjon/, , retreived: 13 January, 2023.

The Norwegian governments official website: www.Regjeringen.no

United Nations Office on Drugs and Crime, “money Laundering.” Accessed 01.03.23. https://www.unodc.org/unodc/en/money-laundering/overview.html

Økokrim.no, «ofte stilte spørsmål». Accessed: 20.03.23. https://www.okokrim.no/ofte-stilte-spoersmaal.549336.no.html