VILNIUS UNIVERSITY
BUSINESS SCHOOL

SUSTAINABLE CORPORATE FINANCE AND INVESTMENTS PROGRAMME

Karolina Rutkauskaitė

THE FINAL MASTER'S THESIS

PINIGŲ PLOVIMO PREVENCIJOS IR DUOMENŲ APSAUGOS SĄNAUDOS ĮMONĖS VEIKLOJE, JŲ REIKŠMĖ IR MAŽINIMO GALIMYBĖS	***AML AND DATA PROTECTION COSTS IN THE FIRMS ACTIVITIES, THEIR SIGNIFICANCE AND OPPORTUNITIES FOR REDUCTION***

Student _____
(signature)

Supervisor_____
(signature)

part.doc. Petras Dubinskas
(Name, surname, academic title, scientific degree of the supervisor)

Vilnius, 2023

SUMMARY

VILNIUS UNIVERSITY BUSINESS SCHOOL

Sustainable Corporate Finance and Investments

Karolina Rutkauskaitė

AML AND DATA PROTECTION COSTS IN THE FIRMS ACTIVITIES, THEIR SIGNIFICANCE AND OPPORTUNITIES FOR REDUCTION

Supervisor – part. doc. Petras Dubinskas

Master's thesis was prepared in Vilnius, in 2023.

Scope of Master's Thesis – 70 pages

Number of tables used in the FMT – 8 pcs.

Number of figures used in the FMT – 6 pcs.

Number of bibliography and references – 73 pcs.

The FMT described in brief:

This thesis explores the problem significant costs of implementing anti-money laundering (AML) and data protection practices for regulated industries. The objective is to assess the importance of these costs and identify potential strategies for reduction. Surveying 54 companies across 14 countries and 19 industries, the study used both qualitative and quantitative methods. Multiple regression models revealed crucial insights: 1) A company's size has a notable linear relationship with allocated AML and data protection costs; 2) Higher awareness levels correlate with increased costs, while investments in data protection lead to reduced expenses; 3) Data protection costs positively correlate with AML costs, indicating synergy between the two. The qualitative phase emphasized AML compliance challenges, focusing on regulations and costs, while data protection measures revealed widespread use of encryption and employee training. Addressing a small response rate, future research should collect more respondents and expand the sample size. Investigating trends over time and integrating qualitative methods like interviews would enhance understanding and findings.

SANTRAUKA

VILNIAUS UNIVERSITETO VERSLO MOKYKLA

Tvarūs Verslo Finansai ir Investicijos

Karolina Rutkauskaitė

PINIGŲ PLOVIMO PREVENCIJOS IR DUOMENŲ APSAUGOS SĄNAUDOS ĮMONĖS VEIKLOJE, JŲ REIKŠMĖ IR MAŽINIMO GALIMYBĖS

Darbo vadovas – part. doc. Petras Dubinskas

Magistro darbas buvo parengtas Vilniuje, 2023m.

Magistro darbo apimtis – 70 puslapiai

Naudotų lentelių skaičius magistro darbe – 8 vnt.

Naudotų paveikslėlių skaičius magistro darbe – 6 vnt.

Šaltinių skaičius magistro darbe – 73 vnt.

Trumpas Magistro darbo aprašymas:

Šiame darbe nagrinėjami kovos su pinigų plovimu ir duomenų apsaugos praktikos įgyvendinimo reguliuojamose pramonės šakose kaštai. Šio darbo tikslas – įvertinti šių išlaidų svarbą ir nustatyti galimas mažinimo strategijas. Apklausoje dalyvavo 54 įmonės iš 14 šalių ir 19 pramonės šakų. Tyrime buvo naudojami tiek kokybiniai tiek kiekybiniai metodai. Daugybinės regresijos modeliai atskleidė esmines įžvalgas: 1) įmonės dydis turi tiesinį ryšį su pinigų plovimo prevencijos ir duomenų apsaugos išlaidomis; 2) didesnis įmonių suvokimas apie pinigų plovimo prevenciją koreliuoja su padidėjusiomis išlaidomis, o investicijos į duomenų apsaugą sumažina išlaidas; 3) duomenų apsaugos išlaidos teigiamai koreliuoja su pinigų plovimo prevencijos išlaidomis, o tai rodo šių dviejų sinergiją. Kokybiniame etape buvo analizuojami didžiausi pinigų plovimo prevencijos iššūkiai, daugiausiai dėmesio skiriant taisyklėms ir išlaidoms, o duomenų apsaugos priemonės atskleidė, kad įmonės plačiai naudoja duomenų šifravimą ir darbuotojų mokymą. Atsižvelgiant į žemą atsakymų skaičių, tolimesni tyrimai turėtų surinkti daugiau respondentų ir išplėsti imties dydį. Tiriant tendencijas per didesnę laiko dalį ir integruojant platesnius kokybinius metodus, kaip interviu, padidėtų temos supratimas bei išvados.

ACKNOWLEDGMENTS:

Gratitude is extended to Mr. Douglas Wolfson, Senior Director, APAC Sales at LexisNexis Risk Solutions, for the provision of the TCOC report, a substantial contribution to enhancing the depth and scope of this research. His professional insights and support have been integral to the development of this thesis.

Appreciation is also conveyed to Dr. William Scott Grob, CAMS-FCI, CGSS, FRM, CAIA, Director – Research & Analysis, for his assistance in the preparation and guidance provided before the research process. His expertise has significantly enriched the scholarly content and rigor of this work.

Special acknowledgment is reserved for the thesis supervisor, part. doc. Petras Dubinskas, whose expert advice, insightful commentary, and consistent guidance have played a crucial role in shaping the trajectory of this research.

TABLE OF CONTENTS

INTRODUCTION 8

1. THEORETICAL FRAMEWORK: AML AND DATA PROTECTION PERSPECTIVES 10

1.1. AML Principles and the History of Money Laundering 10

1.2. Recommendations of the Financial Action Task Force 17

1.3. Importance and Theoretical Foundations of Data Protection 19

1.4. Costs Associated with Anti-Money Laundering 22

1.5. Costs Associated with Data Protection 25

1.6 Opportunities for Cost Reduction in Anti-Money Laundering and Data Protection Measures 29

2. METHODOLOGY 33

2.1. Survey Methodology and Data Collection 34

2.2 Models for AML and Data Protection Costs 38

3. ANALYSIS OF THE RESULTS 42

3.1. Questionnaire survey demographics 42

3.2. Quantitative Approach Results 45

3.3. Qualitative Approach 59

4. CONCLUSIONS AND RECOMMENDATIONS 69

REFERENCES 71

ANNEXES 78

LIST OF TABLES

Table 1. *NACE Industry Sections*…….....34
Table 2. *Country Selection*……...36
Table 3. *Breakdown of reported industries, N=54*……...42
Table 4. *Multiple Regression results, AML Costs*……45
Table 5. *Multiple Regression without dummy variables results, AML Costs*……...48
Table 6. *Multiple Regression results, Data Protection Costs*……...51
Table 7. *Multiple Regression without dummy variables results, Data Protection Costs*.....56
Table 8. *Data Breaches and Security Incidents in the past 2 years. Results distribution. N=54*……65

LIST OF FIGURES

Figure 1. *Stages of Money Laundering and Financing of Terrorism*…….…..….11
Figure 2. *Country distribution of respondents in a survey, N=54*……...42
Figure 3. *AML Compliance Challenges*……...……59
Figure 4. *Top 5 Drivers for Financial Crime Compliance Costs*…….61
Figure 5. *Data Protection Measures. N = 54*……..…….……64
Figure 6. *Reduction of data protection costs. N = 54*……..67

INTRODUCTION

Anti-money laundering and data protection are critical components of efforts to combat money laundering, terrorist financing, and other financial crimes, which pose significant risks to global financial systems and stability.

The **problem** thesis investigates that the costs associated with implementing and maintaining robust anti-money laundering and data protection practices can be substantial for companies operating in regulated industries. Therefore, it is essential to evaluate the significance of these costs and explore the opportunities for their reduction. The **objective** of the thesis is to examine the importance of evaluating anti-money laundering and data protection costs in the context of companies' activities, highlighting their significance, and identifying potential strategies for cost reduction. It is an important topic to dig deep as by thoroughly understanding the nature and magnitude of anti-money laundering and data protection costs, organizations can identify opportunities for reduction and optimize their resource allocation.

The thesis employs and combines both qualitative and quantitative approaches to understand the magnitude of the costs organizations spend to be compliant with anti-money laundering and data protection regulations in certain jurisdictions. The thesis surveys 54 companies and compares the results between 14 countries and 19 industries to get a deep understanding. Furthermore, survey results are compared between different industries to investigate how compliance costs differ and which industries are affected mostly. Companies included in the survey also are separated by asset size to attain a comprehensive insight.

By conducting a survey, it investigates the types of compliance measures in place, the annual cost of implementation and maintenance, the measurement of program effectiveness, the impact of recent regulatory changes, efforts to reduce compliance costs, challenges faced, and strategies for staying updated on regulatory changes and ensuring compliance. These questions highlight the key areas of inquiry regarding the company's compliance practices and their alignment with anti-money laundering and data protection regulations.

By doing so, this research contributes to the understanding of effective risk management, compliance, and operational efficiency in the ever-evolving landscape of regulatory requirements and data privacy concerns. Shedding light on these aspects, the thesis

aims to provide valuable insights and recommendations to enhance compliance, minimize risks, and promote sustainable business practices.

This thesis is organized as follows – section one analyzes the scientific literature, which encompasses five main areas. Firstly, it examines the significance and theoretical underpinnings of anti-money laundering measures. Secondly, it explores the importance and the theoretical foundations of data protection. The analysis of scientific literature also includes a discussion on the costs associated with anti-money laundering and separately with data protection. Furthermore, it investigates the potential opportunities for reducing these costs. Moreover, section two presents the methodology used in this analysis. The survey parameters and specifics of the selection of the companies are described. Section three portrays the results, where the main findings are presented and discussed further. Finally, section four concludes and describes the limitations of the research as well as elaborates on the possible areas for further research.

1. THEORETICAL FRAMEWORK: AML AND DATA PROTECTION PERSPECTIVES

1.1. AML Principles and the History of Money Laundering

Anti-money laundering (AML) is a crucial process that financial institutions and governments implement to prevent money laundering, terrorism financing, and other illegal financial activities. There is a significant amount of discussion, regarding the importance of anti-money laundering and data protection, and its impact on society in scientific literature.

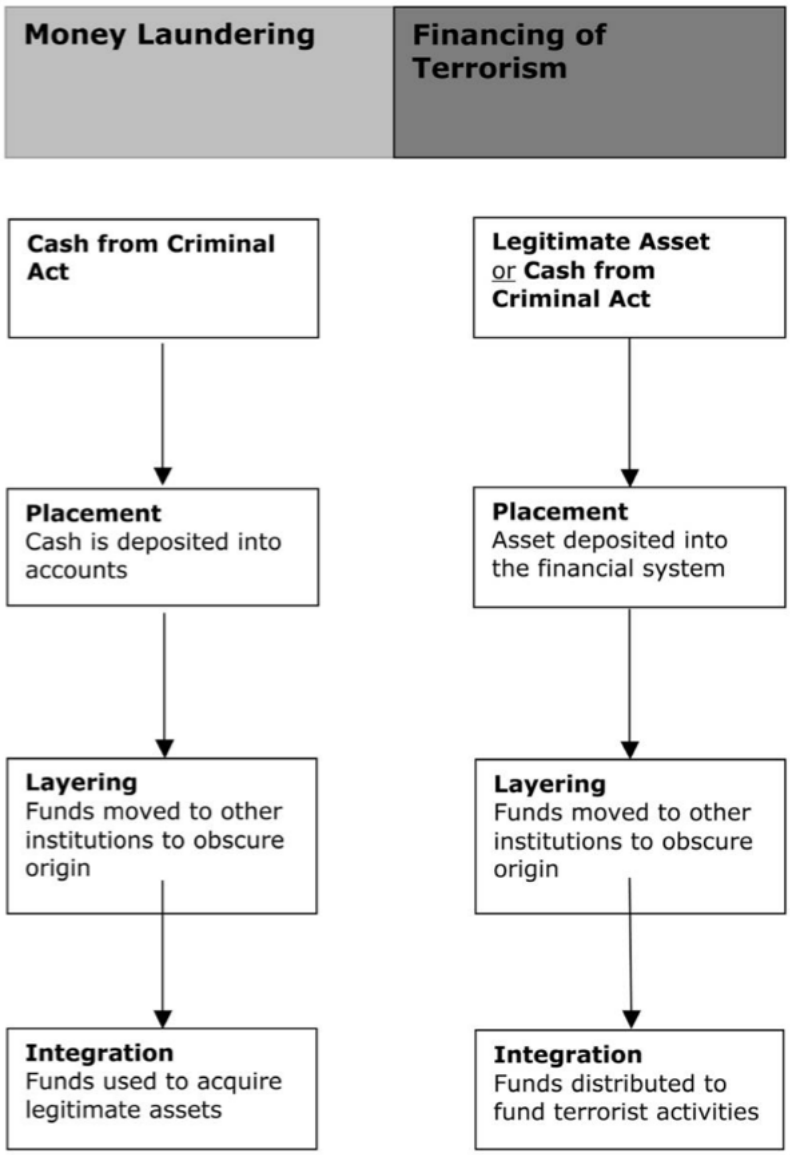
Analyzing the scientific literature on the topic of anti-money laundering and data protection costs to companies is important as it helps to identify challenges the companies face in complying with anti-money laundering and data protection regulations. Furthermore, the analysis of scientific literature could identify potential gaps, which would contribute to the development of strategies for reducing costs spent by the companies for them to be compliant.

Wheeler (2023) describes anti-money laundering as a set of measures, including regulations, laws, and protocols, designed to prevent and detect the conversion of illegally obtained funds into legitimate income. Anti-money laundering policies are critical for banks and other financial institutions as they help combat financial crimes. To comply with AML regulations, banks are required to gather customer information, supervise, and examine their transactions, and notify financial regulatory agencies of any questionable activities. Furthermore, the AML holding period mandates that deposits stay in an account for a specific period (typically at least five trading days in the U.S.). This holding period may be used by banks to assist in anti-money laundering and risk management. (Wheeler, 2023)

However, to understand the importance of AML and delve deeper into its origins it is important to elaborate on the literature that investigates how money laundering works. Levi & Reuter (2006) identify three money laundering stages – placement, layering, and integration.

Figure 1

Stages of Money Laundering and Financing of Terrorism



Source: Levi and Reuter, 2006, p. 313

Placement refers to the process of introducing funds into the financial system, which can be accomplished through simple methods such as cash deposits or more intricate methods. Mohammad et al., (2022) describe placement, the initial stage of money laundering as the most critical and exposed step in the process of laundering illegal funds. According to the research paper, the primary objective of the placement stage in money laundering is to infuse illegally obtained funds into the financial system without arousing suspicion from financial institutions

or government authorities. Criminals use various techniques such as depositing funds that are below the financial institution's reporting threshold or mixing legally obtained cash deposits with illegally obtained funds. Elaborating further, another method of achieving the placement process is through money trafficking, which involves the illegal transportation of physical cash and financial instruments across borders. Other methods include exploiting gaps in banking regulations to carry out transactions, use of currency exchange (in underdeveloped countries) that lack supervision from the authorities, use of brokers of securities, or setting up shell corporations.

Going further, the second stage of money laundering according to Levi & Reuter (2006) is layering. This is a process that aims to create a complex trail that makes it difficult to trace the funds back to their illegal source. Jendruszak (2023) states that layering is a series of complex financial transactions aimed at distancing illicit funds from their source and creating a web of transactions that makes it difficult to trace the money's criminal origins. This stage typically involves multiple transactions through various accounts and across different financial institutions, often in different countries, making it challenging for law enforcement agencies to follow the money trail. According to the author examples of the layering stage could include setting up shell companies (entities that are set up to conceal the illicit activities resulting from the laundering of money), asset investments- investing in expensive artwork or real estate, which appears legitimate is a common technique used to hide or distribute large amounts of laundered money. Furthermore, the use of accomplices – corrupt employees in the banking sector or even those who participate in the process unknowingly could help store and exchange the money that is being laundered. ComplyAdvantage (2019) provides an example of how the layering stage could look in practice – multiple times customers would withdraw small amounts of cash from the accounts, where illicit funds were placed during the first stage of the money laundering process. Each cash withdrawal would be small (lower than the threshold of the financial institution, where the funds are kept). The cash would then be wired to an offshore account, consolidated, and used to buy expensive items e.g., yachts or artwork.

The third and final stage of money laundering according to Levi & Reuter (2006) is integration. A research paper by Johari et al. (2020) describes this last stage as a process where the illegally obtained funds are introduced into the legitimate economy as clean money, usually by purchasing high-value assets (property, luxury items). Another option to introduce illegal

money into the market is via engaging in legal business activities. Detection of illicit funds at this stage is challenging as they appear to come from lawful sources.

Furthermore, it is essential to delve deeper into money laundering theories and origins to understand the motivation behind money laundering as a concept and its rationale. DesJardins (2013) distinguishes several business ethics theories that could explain the reasoning behind money laundering. The first one is individualism theory, which emphasizes rights and certain freedoms that an individual might have and prioritizes them over those of a group or even society as a whole. It relates to money laundering in the sense that businesses should be free to pursue their interests (i.e., maximizing profits) without being obligated to consider broader social implications for their actions. Furthermore, DesJardins (2013) discusses utilitarian theory, which emphasizes the importance of maximizing overall happiness and or well-being. According to this theory, the right action to take is the one that would provide the largest extent of happiness for the most significant number of people. For instance, when applying utilitarian theory businesses may argue that engaging in illegal money laundering activities will allow them to conduct tax evasion in that sense increasing businesses' competitiveness, which could lead to greater profits. In addition, DesJardins (2013) explains that Kantianism theory developed by Immanuel Kanthem claims that individuals have inherent value and should be treated with the utmost respect and dignity. Mohammad et al., (2022) explain that persons or businesses selfishly engage in money laundering acts, disregarding the well-being of all parties involved as well as lacking goodwill. Moreover, their actions violate the three formulas described by the Kantianism theory – universal law, humanity, and autonomy. Going further, the virtue theory described by DesJardins (2013) is a moral foundation that emphasizes the importance of developing virtuous character traits, such as honesty, fairness, and compassion. When looking into the context of business ethics it can be applied to a fact that whether businesses have a responsibility to act with integrity or whether they only should obey the law. Businesses that engage in money laundering demonstrate a lack of virtuous character traits such as honesty, integrity, and respect for the law. On top of that DesJardins (2013) explains the story of “The Boy Who Cried Wolf” – the famous parable that aims to illustrate the importance of credibility and integrity, - the crying wolf theory. Like how the boy in the tale lost the confidence of his community by constantly making untrue statements, companies that participate in unethical or dishonest conduct risk ruining their credibility and losing the trust of those invested in their success. This relates greatly to money laundering as this illegal activity can erode the trust and confidence of stakeholders in the

financial system. Finally, the agency theory described in this research relates to money laundering rationale as it highlights the possibility for agency problems that may occur when agents (e.g., managers of a company) act by principals that are not aligned, and they could prioritize their interests over for instance company's shareholders. In case of money laundering agents might engage in illegal activities that could benefit them personally at the expense of a company.

Anti-money laundering traces back and originates from 1970 when the Bank Secrecy Act was issued. Up until now, it has become a vital instrument in combating money laundering. According to the Financial Action Task Force (n.d.), the law established obligations for individuals, banks, and other financial institutions to maintain records and submit reports. The objective of the law was to aid in the detection of the origin, amount, and transfer of currency and other forms of monetary assets entering or leaving the United States or being deposited in financial institutions. The Bank Secrecy Act mandated that banks fulfill three requirements. The first requirement that banks were obligated to do was to submit a Currency Transaction Report for cash transactions exceeding $10,000. The second requirement was to accurately identify the individuals conducting the transactions. Finally, the third requirement obligated banks to create and preserve suitable records of financial transactions to maintain an audit trail. Bank Secrecy Act was the law that set the foundation for the financial crime prevention framework.

Following that the Anti-Drug Abuse Act of 1988 came into play. Gurule (1995), describes that the aim of the Money Laundering Control Act of 1986 was to criminalize the act of concealing and investing illicit profits generated from criminal activity as a new federal offense. The legislation focuses on behavior that takes place after the initial crime. According to the Financial Action Task Force (n.d.), the Money Laundering Control Act established money laundering as a federal crime. Furthermore, the law made it illegal to organize financial transactions in a way that avoids the need to submit Currency Transaction Reports (CTRs) as well as established the concept of civil and criminal forfeiture for breaches of the Bank Secrecy Act (BSA). Finally, the law instructed banks to develop and maintain processes to confirm and supervise compliance with the reporting and record-keeping obligations of the Bank Secrecy Act (BSA).

Afterward, the Anti-Drug Abuse Act of 1988 took effect. Financial Action Task Force (n.d.), describes that this law broadened the scope of financial institutions to include professions like car dealers and real estate closing personnel and mandated that they report significant currency transactions. Additionally, it made it obligatory to verify the identity of individuals buying monetary instruments valued above $3,000. Following this, Annunzio-Wylie Anti-Money Laundering Act (1992) became active. ComplyAdvantage (2021) defines that this act enhanced the penalties for breaking the Bank Secrecy Act (BSA) and granted financial institutions and their staff immunity from civil responsibility in the occurrence of disclosing any known or suspected criminal acts or suspicious activity. In addition, according to the Financial Action Task Force (n.d.), the law mandated that wire transfers must undergo verification and record-keeping processes. Additionally, it established the Bank Secrecy Act Advisory Group (BSAAG). A Notice by the Financial Crimes Enforcement Network (2023) describes BSAAG as a channel for the Treasury to obtain counsel on the reporting obligations outlined in the Bank Secrecy Act (BSA), and the channel that also educates representatives from the private sector on how the data they submit is utilized.

In 1994 the Money Laundering Suppression Act became active. Financial Action Task Force (n.d.), describes that law obligated banking agencies to assess and upgrade their training frameworks and to further upgrade anti-money laundering examination methods. Moreover, the law mandated that institutions in the banking sector must review their methodology for referring cases to the appropriate law enforcement authorities. In addition, the Money Laundering Suppression Act simplified the process for exceptions when allocating Currency Transaction Reports (CTRs). Additionally, the law made it mandatory to register Money Services Business (MSB) as an owner or controlling person and keep a list of authorized agent businesses. Also, unregistered MSB started to be treated as a federal offense. Finally, the Money Laundering Suppression Act recommended that all the states would adopt uniform laws that would apply to MSBs.

Following that, in 1998 Money Laundering and Financial Crimes Strategy Act took place. Financial Action Task Force (n.d.), states that the law mandated banking agencies to establish anti-money laundering training programs for their examiners. It also directed the Department of the Treasury and other agencies to devise a National Money Laundering Strategy. Moreover, it established the High-Intensity Money Laundering and Related Financial Crime Area (HIFCA) Task Forces, which would concentrate law enforcement efforts across

federal, state, and local levels in areas where money laundering is widespread. HIFCAs according to the Money Laundering and Financial Crimes Strategy Act could either be defined geographically or could be created to tackle money laundering in a specific industry sector, financial institution, or group of financial institutions.

Finally, going into the XXI century the Financial Action Task Force (n.d.), explains that in 2001 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) was established. Three years later, the Intelligence Reform & Terrorism Prevention Act of 2004 came into effect. The USA PATRIOT Act made it illegal to finance terrorism and enhanced the existing BSA framework by requiring stronger customer identification procedures. It prohibited financial institutions from doing business with foreign shell banks and required them to have due diligence procedures in place, including enhanced procedures for foreign correspondent and private banking accounts. The act also improved information sharing between financial institutions and the government, requiring both government-institution information sharing and voluntary information sharing among financial institutions. Additionally, it expanded the anti-money laundering program requirements to all financial institutions, increased civil and criminal penalties for money laundering, and provided the Secretary of the Treasury with the authority to impose "special measures" on jurisdictions, institutions, or transactions that are of "primary money laundering concern." The act facilitated records access and required banks to respond to regulatory requests for information within 120 hours. Finally, it required federal banking agencies to consider a bank's anti-money laundering record when reviewing bank mergers, acquisitions, and other applications for business combinations. Furthermore, the Intelligence Reform & Terrorism Prevention Act directed the Secretary of the Treasury to create rules mandating that specific financial institutions report electronic transfers of funds across international borders if such reporting is deemed necessary to combat money laundering and terrorism financing.

In conclusion, the analysis of AML principles and the historical development of money laundering reveals a significant role of AML in combating financial crime. Furthermore, exploring money laundering theories sheds light on the ethical perspectives driving such activities within the companies.

1.2. Recommendations of the Financial Action Task Force

Building upon this foundation, the following section delves into the key standards established by the Financial Action Task Force. Understanding these international recommendations is essential for a comprehensive analysis of AML and data protection costs.

The Financial Action Task Force (FATF), formed in 1989 is an intergovernmental policy-making organization whose missions are to develop and advocate national and worldwide regulations to prevent money laundering and the funding of terrorism. In general members of FATF (currently FATF is comprised of 37 full members including the European Commission) explain their goal to ensure overall financial integrity (Nance, 2018).

The FATF has established standards called FATF Recommendations, which provide governments of different jurisdictions with ways to combat money laundering, and financial crime, combat terrorist financing, and tax evasion, increase the number of weapons used for mass destruction purposes, and corruption (Financial Action Task Force, n.d.). It is important to delve deeper into FATF Recommendations as they provide clear frameworks for AML compliance and guidance to effective measures of reduction for costs for financial institutions. When looking at the FATF Recommendations (2012-2023) there are 40 subsections all relating to various measures. The first one is (Anti-Money Laundering/Counter Terrorist Financing) AML/CTF policies and coordination, which consists of an assessment of risk and risk-based approach application and national cooperation and coordination. According to this first section, a risk-based approach is of the utmost importance and should be treated as a foundation for risk-based measures when combating money laundering and terrorist financing. Furthermore, countries should evaluate and assess risks for the country and act accordingly based on the risk assessed (if it is high or low). Following this, countries should have policies that should be followed on a national level, they should establish an authority that would be responsible for reviewing and coordinating such policies. The Second section of recommendations involves money laundering and confiscation, which consist of money laundering offenses and confiscation and provisional measures. This recommendation suggests that countries should criminalize money laundering according to the Vienna and Palermo Conventions as well as adopt various measures that would enable authorities to freeze or confiscate e.g. laundered property. The third section called terrorist financing and Financing of proliferation includes points regarding terrorist financing offenses, targeted financial sanctions related to terrorism

and terrorist financing, targeted financial sanctions related to proliferation, and non-profit organizations. This section of recommendation mostly covers the need to criminalize terrorist financing and the implementation of financial sanctions, which would comply with United Nations Security Council resolutions that would target both terrorist financing and the proliferation of weapons for mass destruction. Furthermore, this section covers the non-profit organization issue, explaining how countries should implement needed measures to protect them from terrorist financing. Another section of recommendation called preventive measures covers customer due diligence and record-keeping, additional measures for specific customers and activities, reliance, controls, and financial groups, reporting of suspicious transactions, and designated non-financial businesses and professions. Looking at customer due diligence companies in the financial sectors should be obliged to conduct customer due diligence when establishing business-related relationships, in cases where there could be money laundering occurrence or if there are indications that data of the customer was collected in an inadequate manner as well as for carrying transactions above 15,000 EUR/USD. Companies operating in the financial sectors should also keep relevant records with the minimum timeframe being 5 years as well as allow access to these records for any relevant authorities. Furthermore, financial institutions should be obligated to identify if their customers are Politically Exposed Persons (PEPs) and have relevant procedures (employing a high-risk approach) when handling such customers. In addition, financial companies should be kept informed about respondent institutions when referencing cross-border correspondent banking, assessing their AML/CTF controls, gathering efficient data about their nature of business and their responsibilities as well as making sure that respondent banks conducted customer due diligence on their customer as well. Financial institutions based on this recommendation should also be informed about money service providers they would need to make sure that those institutions are properly licensed and compliant with FATF recommendations. Furthermore, companies in the financial sector should be aware of the money laundering and terrorist financing risks when there are newly developed technologies or products launched as well as monitoring wire transfers to make sure there is sufficient information available to prevent any risks of incompliance. Financial institutions might be prohibited from relying upon the information of third parties conducting customer due diligence if certain criteria are not being followed. In addition, financial institutions would have to make sure that the same regulations would apply to any other foreign branches and be perform enhanced due diligence on customers operating within high-risk countries, and be responsible for reporting any suspicious transactions, and cases of possible tipping-off. Further section regarding transparency and beneficial ownership of legal

persons and arrangements encourages countries to employ needed measures to prevent money laundering when these instruments may be misused. The section regarding the powers and responsibilities of competent authorities recommends that countries should ensure that financial institutions are supervised regularly. The last section covers international cooperation, where countries are obliged to implement all the relevant international conventions as well as provide mutual legal assistance to a high extent and cooperate internationally concerning money laundering offenses.

Overall, these recommendations signify the international commitment to combat financial crime. These standards, spanning various sections and measures provide a comprehensive framework for countries to adopt in their efforts to enhance financial integrity. Recommendations emphasize risk-based approaches, various preventive measures, and international communication and cooperation, which reflects the dynamic nature of combating the always-changing and evolving financial threats.

1.3. Importance and Theoretical Foundations of Data Protection

Progressing forward with the review of scientific literature analysis of this research it is important to investigate the topic of data protection. To start with, it is essential to investigate the importance of data protection aspect for customers and businesses.

Hoofnagle et al. (2019) describe that the European Union's General Data Protection Regulation (GDPR) is so crucial that when dealing with personal data every aspect is required to have careful planning present. Wolford (n.d.) describes that GDPR became active as a regulation on May 25, 2018. The history of GDPR according to the author started in 1995 when European Data Protection Directive adopted by the European Union came into effect, which established what should be the minimum standards for data protection and security. Each state of the EU then applied and implemented its laws considering this directive. (Lord, 2022) describes that the Data Protection Directive has a foundation of seven principles. The first, notice, states that individuals should be notified whenever their data is being collected. Second, purpose, pronounces that personal data should only be used for the express purpose for which said data was acquired. The third one, consent describes that an individual's consent should be collected always when their data is being shared with other parties. Furthermore, the fourth principle speaks about the security of data – all the collected personal data should be held

securely against abuse and or compromise. The fifth principle called disclosure claims that data collectors should disclose to individuals when their data is being collected. Moreover, the sixth and seventh principles called access and accountability respectively declare individuals should have direct access and the possibility to correct any inaccuracies in their data and finally, there should be a means for individuals to hold those who acquire their data accountable for the above mentioned six principles. European Data Protection Supervisor (n.d.) describes that after Directive 95/46/EC (the European Data Protection Directive) was implemented, in 2012 the European Commission suggested a complete overhaul of before mentioned European Data Protection Directive to enhance the rights of online security and privacy as well as promote the digital Economy in Europe. Following that European Union. European Data Protection Supervisor (2012) released a statement where the entity supports the proposed reforms, however, recommends making several adjustments to strengthen privacy rights further. The European Data Protection Supervisor's recommendations included a more comprehensive definition of the scope of personal data. Furthermore, it ensures individuals' rights to their own disclosed data, taking measures to strengthen data protection authorities' independence and cooperation, and reinforcing sanctions for data breaches. Moreover, the European Data Protection Supervisor emphasizes the importance of including measures to enhance data portability, data protection impact assessments, and codes of conduct for data controllers. The recommendations also elaborate on the significance of user education and the engagement of the reform process. In 2014, the European Parliament demonstrated strong approval, with overwhelming support by voting, and the General Data Protection Regulation was adopted in 2016 and became effective on 25 May 2018. (European Data Protection Supervisor, n.d.)

Zaeem & Barber (2020) discuss the impact of the GDPR on privacy policies. According to the authors, the GDPR is based on several key principles, which include lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality (security), and accountability. Although the GDPR is a legal framework established by the European Union, it applies to any entity that collects or handles the personal information of EU citizens, regardless of where that entity is based or operates. The findings suggested that most privacy policies were able to satisfy many but not all GDPR requirements, with the most notable non-compliance being the lack of transparency and explicit disclosure of processing and protection of consumer personal information. While changes have been made to privacy policies to improve compliance, there has been a decrease in protection for factors

such as sharing with law enforcement and deleting/editing information by 8% and 13% respectively.

Hoofnagle et al. (2019) discuss the strategic implications of the GDPR. The authors highlight eight key implications of the GDPR. The first one is that the GDPR serves as a data governance framework because it encourages companies to plan for the collection, use, and destruction of the collected data. Furthermore, it can also cause businesses to recognize the value of the data as a strategic asset. Second, GDPR requires companies to take privacy. As seriously as other important laws such as those related to, for instance, foreign corrupt practices. This is because GDPR has strict penalties and requires companies to notify individuals of any security incidents. Therefore, executive officers are discouraged from treating privacy violations as minor issues. In addition, GDPR requires companies that use personal data to make sure that service providers also follow the rules of privacy. This applies to both the company itself and any other parties involved in handling the data. The regulation also gives more power to certain officials in the companies, also called data Protection Officers, who must keep records of what happens to the data and report any data breaches. Additionally, the GDPR sets high standards for consent, which indicates that companies cannot use personal data without clear and informed consent from the involved people. What is more, the GDPR values accuracy in personal data and elaborates that individuals should be involved in decisions about their data. Preferably, there should be direct relationships between individuals and the companies that they share their data with, excluding third parties. According to the authors, this could lead to the establishment of a new type of company that would help individuals manage their data. Finally, the research paper explains that companies may struggle with strict GDPR requirements and mistakes could be made. This could lead to conflicts between large companies and authorities over how the GDPR should be interpreted and enforced.

To conclude, the exploration of data protection, particularly within the context of EU GRPR regulations, reveals the significance for companies to protect the personal information of their customers. The principles of lawfulness, fairness, transparency, and accountability form the foundation of GDPR, which influences privacy policies and strategic considerations for companies greatly.

1.4. Costs Associated with Anti-Money Laundering

There is a significant amount of scientific literature discussing the costs of AML compliance to the private sector. Many studies have analyzed the financial burden of AML compliance on banks and other financial institutions as well as the effectiveness of AML regulations in preventing money laundering and terrorist financing.

LexisNexis Risk Solutions (2022) surveyed 5 Asia-Pacific (APAC) markets – China, India, Malaysia, Japan, and Australia. 5 major findings were described in this survey. The first one was that compliance costs related to financial crime are considerably higher for larger financial institutions in the Asia-Pacific region. According to the survey, this is primarily due to the growing regulatory landscape in anti-money laundering, increasing geopolitical risks, and the constantly evolving tactics of criminals engaged in financial crimes. The estimated cost of financial crime compliance for financial institutions in APAC countries is $50.1 billion. The largest part comes from large banks, which contribute to these expenses around 80% ($40.8 billion). When looking at countries more specifically, China and Japan have the highest overall total costs of financial crime compliance, with $21.8 billion and $17.9 billion respectively. The main reason for that is due to the presence of numerous financial institutions in these countries. The financial institutions based on this report provided the main drivers of increased costs of compliance – the largest one overall was investing in new technologies, data, and or tools. Following this, investments in risk assessments, staffing costs, and investigations are more complex. The second finding of the survey was that financial institutions in the APAC region are facing a rising threat of diverse financial crimes, encompassing areas such as digital payments, cryptocurrency, involvement of third parties, and the illicit movement of illicit funds. According to the survey, the utilization of money mules to launder illicit proceeds emerges as a primary factor contributing to the escalation of compliance expenses for numerous banks and investment firms in the APAC region. The third finding describes that APAC financial institutions, as well as investment and asset management firms, face challenges in compliance screening, especially in Know Your Customer (KYC) part–account onboarding as well as accurately identifying PEPs and conducting regulatory reporting. This relates to 4th finding of this survey – that COVID-19 harmed the productivity and compliance monitoring capabilities of financial institutions in the APAC region. The last finding suggests that in the investigated APAC region, financial institutions that invest in a higher proportion of their

financial crime compliance costs in compliance technology encounter fewer significant disruptions in terms of cost and operational efficiency related to compliance.

LexisNexis Risk Solutions (2016) survey elaborates on the average cost of AML compliance based on the size of the firm. The statistics were estimated in the Asia market as well. Smaller financial institutions, with assets below US$1 billion, reported an average AML operational cost of approximately US$850,000. Mid-tier companies had an average expense of US$7.4 million, while larger top-tier firms, with assets exceeding US$100 billion, spend an average of US$15.8 million annually on AML compliance. When comparing two surveys of 2022 and 2016, in both cases China had the highest collective average of AML operational costs, primarily driven by the presence of numerous large banks within the respondent pool of Chinese firms. Similarly, when looking at different operational components of AML compliance within firms and comparing two surveys results could also be interpreted as similar. In a 2016 survey, collectively, activities related to watchlists, which include KYC processes, periodic screening, and sanctions operations, constitute 33% of AML compliance costs. In contrast, the costs attributed to transaction monitoring analysis represent only 9% of the total expenses.

A global survey conducted by LexisNexis Risk Solutions (2021) encloses 4 regions – Asia-Pacific (APAC) discussed previously, Europe, the Middle East and Africa (EMEA), Latin America (LATAM), and North America. The survey represents banks, investment firms, asset management firms, and insurance firms. Globally, the report finds that the projected total costs of financial crime compliance constituted $213.9 billion. The key finding of the report suggests that the majority of total projected costs for financial crime compliance are attributed to Western European Countries and the United States, accounting for 82.7% of the overall costs. Among them, Germany and the United States experience the largest increases in costs, with Germany leading by a substantial margin. The cost increase in Germany amounts to $9.6 billion, while the United States follows closely with a cost increase of $8.8 billion. According to the paper by Friedrich & Quick (2019), Germany is evaluated as largely compliant with FATF Recommendations, with remaining issues to improve – supervision and guidance of the non-financial sector institutions. According to LexisNexis Risk Solutions (2021), one notable shift in the distribution of these costs is towards labor expenses, which can be attributed to factors such as increased hiring or contracting higher volumes and risks during the COVID-19 pandemic. The paper also elaborates on the fact that North America and LATAM encountered

substantial cost escalations, which were attributed to the effects of the COVID-19 pandemic. Areas that were most affected consisted of heightened volumes of alerts and suspicious transactions, inefficiencies in resolving alerts and conducting due diligence, an increase in reliance on alert resolution, limitations in performing accurate risk profiling, sanctions screening, and identifying PEPs. Ilahi & Widowaty (2021) emphasize that during the COVID-19 period looking specifically at the period from 2019 to 2020 39.6% of respondents according to the Indonesian Survey Institute responded to notifying a significant increase in corruption, and money laundering in Indonesia. Looking at the region of Europe, more specifically in Poland, Gryszczyńska (2021) explains that Covid-19 inflated the amount of money laundering and financial crime taking place online. According to the author, in 2020 42% of proceedings were identified as "online" crimes in the police databases in Poland. It is also important to mention that in the realm of cybercrime with a focus on monetary gains money laundering stands out as the predominant underlying offense.

Revisiting the report of LexisNexis Risk Solutions (2021) the additional finding suggested that compliance cost increase in the Europe region could be impacted by the fact that larger Dutch firms have experienced changes in their annual financial crime compliance costs due to the implementation of a centralized transaction monitoring platform by the five largest banks. AML RightSource (2020) elaborates on this collaboration – ING, ABN Amro, Rabobank, Triodos Bank, and Volksbank created a Transaction Monitoring Netherlands (TMNL), which by having access to the aggregated transaction data can identify unusual behavioral patterns that may not be readily apparent when examining the data of each bank. The introduction of this system, according to the article demonstrated the urgent need for Dutch banks to enhance their anti-money laundering procedures and systems as the country was recognized as a significant hub for such illicit activities. The Dutch Banking Association approximated that criminal funds amounted to €16 billion that is being laundered in the Netherlands annually.

Crews (2018) investigates the compliance costs and consequences faced by companies in the United States. To start, the paper emphasizes the fact that compliance creates a significant financial burden – in 2017, for instance, the estimated cost of federal regulations amounted to a significant amount of $1.9 trillion. This amount was estimated by taking not only direct costs of complying with regulations but also indirect costs, such as hiring staff responsible for compliance assurance, implementation of compliance system costs, and costs of documentation

maintenance. According to the paper, the regulatory costs mentioned previously constituted approximately 10% of the United States' gross domestic product, which was valued at around $19.738 in 2017 according to the Commerce Department's Bureau of Economic Analysis. The paper also touches upon the productivity reduction issue that arises from the need to be compliant with the regulations. Compliance requirements often demand businesses to allocate substantial resources and manpower to ensure adherence to regulations. This hinders productivity and takes the focus out of primary objectives - core operations, innovation, and expansion of the companies. Furthermore, the paper elaborates that small businesses may suffer from the complexity of the regulatory frameworks and the high costs and burdens the high compliance costs bring. This complexity disproportionately affects small businesses that may lack the expertise and resources necessary to navigate the regulatory landscape effectively. Small businesses face challenges in meeting regulatory requirements, which diverts resources away from investment in new technologies, research and development, and market expansion.

In conclusion, the examination of costs associated with anti-money laundering emphasizes the substantial financial burden placed on companies and financial institutions. Constantly evolving regulations, geopolitical risks, and the dynamic nature of always-evolving financial crimes contribute to an increase in compliance costs. Variations in different regions, such as Europe and Asia highlight the global impact AML regulation holds. The COVID-19 pandemic further amplified challenges, which affected sanction screening, labor expenses, and necessary adaptions to deal with increased financial crime.

1.5. Costs Associated with Data Protection

Scientific literature also analyses data protection costs. (White, 2020) focuses on assessing the impact of the General Data Protection Regulation on the cost of conducting business. The analysis conducted by the researcher covered a comprehensive examination of 6,960 distinct firms from the European Union and 4,739 companies from the United States during the period 2016-2018. When evaluating staff costs there is a significant difference between companies in the European Union and the United States. On average, European Union companies experienced a substantial increase of 72% in their expenditure on staff costs, whereas United States companies only recorded a modest increase of 17%, during the investigated period.

The period of 2018 was distinctively significant concerning data protection cost increase for businesses as the European Union implemented GDPR in 2018. (Chen et al., 2022) investigate the GDPR effect on the performance of firms globally (across 61 countries and 34 industries). The research utilizes international input-output tables to assess companies' exposure to GDPR. Authors construct a shift-share instrument, by analyzing the shares of output sold to European Union markets for different countries and industries, which interact with dummy variables to capture the GDPR impact from 2018 onwards. The findings of the paper indicate that both cost and sales channels are significant, however, cost channel plays a more significant role. On average, based on findings, companies targeting European Union markets experienced an 8% decrease in profits and a relatively smaller 2% decline in sales. Important to mention that large technology companies were relatively unaffected by the regulation, while small technology companies experienced a more significant negative impact on profits compared to the overall sample. The results of the research indicate the importance of considering compliance costs in understanding the effects of GDPR on businesses. Research also emphasizes the fact that compliance expenses have emerged as the primary factor, which negatively impacts companies. (Jia et al., 2021) aim to assess the impact of enhanced data regulation introduced by the GDPR on the value of venture capital and angel investments in Europe. The findings of the research demonstrate a continued decrease in the number of investment deals in early-stage European technology ventures after the implementation of the GDPR, in comparison to technology ventures in the United States. The research also touches upon the impact COVID-19 had on data protection costs as the pandemic resulted in substantial growth in online user activity, leading to a surge of data generated by individuals and businesses. This increase highlighted the growing conflicts between data protection measures. Based on findings European Union technology firms, when compared to the United States witnessed a significant average decrease of 21.51% in the number of venture investment deals.

Looking at the direct costs of data privacy regulation (Huddleston, 2021) elaborates that they arise and are primarily associated with initial compliance efforts. The author provides that a survey conducted by Big 4 companies – PwC and EY and the International Association of Privacy Professionals in 2017 and 2018 respectively found that 40 percent of participating companies spent more than $10 million on GDPR compliance and annual expenditure of $1.3 million was reported as spent to be compliant with GDPR respectively. This is data taken not only concerning European Union companies but including companies of the United States with a European Union presence. An important aspect discussed by the author mentioned that

additional burden comes from the fact that companies strive to meet the specific GDPR requirements for each jurisdiction. Looking more in-depth at the United States McQuinn & Castro (2019) examine the expenses related to various aspects of data privacy regulations including the appointment of data protection officers, conduction of privacy audits, enhancement of data quality for easier fulfillment of subject requests, costs associated with facilitating user rights such as access, data portability, deletion requests, and data correction. Additionally, the research considers increased legal risks as well as production costs incurred by consumers due to frequent po-up consent notices. Research shows that in terms of compliance procedures, organizations and individuals in the United States would collectively incur annual costs of approximately $18 billion. According to the findings, the largest amount comes from the total expenditure associated with ensuring the provision of rights, such as access, deletion, data portability, and rectification - $7.2 billion. Following this, expenses of updating and managing data infrastructure across all companies in the United States that handle personal data - $5.4 billion. In comparison, the smallest aspect comes from the annual cost of unrestricted access requirements for all organizations in the United States that process personal data – approximately $340 million.

When looking at the significant costs the data protection compliance costs bring, it is important to look at literature investigating the consequences of not following these regulations. Ferwerda (2018) explains that in the field of AML, there are two distinct categories of fines, The first category pertains to preventive measures, where fines are imposed on reporting entities that fail to fulfill their obligations. The second category relates to the repressive aspect of the policy, involving fines imposed on money launderers who have been prosecuted and found guilty. The research study conducted by Ponemon Institute (2022) analyzed 550 organizations that experienced data breaches in the period from March 2021 to March 2022. Investigated breaches occurred in 17 countries and regions encompassing 17 different industries. Research key findings show that in 2022 the average cost of a data breach reached a record high of $4.35 million, marking a 2.6% increase compared to the previous year’s average of $4.24 million. This finding represents a significant increase from the average cost of $3.86 million, reported in 2020. Following that, among the organizations surveyed, a significant majority of 83% had encountered multiple data breaches during the investigated period, with only a small percentage of 17% reporting their first-ever breach. Important to notice that 60% of organizations indicated that they had increased the prices of their services and products as a direct response to the data breach incidents. These findings highlight the

prevalence of repeated breaches and the financial impact they have on businesses, leading to increased costs to consumers.

Research conducted by the Ponemon Institute based on IBM Security (2021) elaborates on the COVID-19 impact on data protection breaches. Breaches that occurred based on research findings show that remote work was associated with an average cost that was $1.07 million higher compared to breaches where remote work was not a contributing factor. Based on findings, around 17.5% of companies reported remote work as a factor in the breach. Furthermore, companies with more than 50% of their workforce operating remotely took 58 days longer to detect and report breaches compared to those with less remote work involvement. Increased costs were led by the implementation of IT solutions, for instance, cloud migration and remote work. Surprising findings elaborate that organizations that did not undertake digital transformation changes due to COVID-19 experienced costs that were $750,000 higher than the global average, representing a difference of 16.6%. In addition, the study shows that for the eleventh consecutive year, healthcare organizations incurred the highest average cost of data breaches. The average cost of healthcare data breaches rose by 29.5% from $7.13 million in 2020 to $9.23 million in 2021. Findings also show that the identification of breaches was a significant factor in increasing costs. On average, it took 287 days to detect and mitigate a data breach. Data breaches that exceeded 200 days to identify and contain resulted in an average cost of $4.87 million, whereas breaches resolved within 200 days had an average cost of $3.61 million.

Overall, the scientific literature shed light on the substantial increase in costs concerning data privacy regulations on businesses globally. An increase in staff costs for EU companies following the implementation of GDPR in 2018, contrasted with the more modest increase observed in the United States. In addition, literature researching non-compliance was touched upon, which emphasized the record-high average cost of data breaches, which signifies the financial burn on companies' data protection compliance and consequently affects the customers as well.

1.6 Opportunities for Cost Reduction in Anti-Money Laundering and Data Protection Measures

Going further with the analysis of the literature it is important to evaluate possibilities of reducing compliance costs as it allows organizations to allocate their resources more efficiently and enhance their competitiveness. To gain insights into effective strategies, it is crucial to investigate the existing scientific literature on compliance cost reduction. Frazzetto (2022) elaborates that artificial intelligence (AI) and advanced automation techniques, for instance, robotic process automation (RPA) and natural language processing (NLP) have the potential to enhance operational efficiencies and reduce costs associated with regulatory compliance. According to the author, one of the examples of how AI can be employed is transaction monitoring. Integrating AI into traditional transaction monitoring systems in financial services could significantly reduce the number of false positives, which can reach as high as 90% and usually are reviewed manually by compliance officers (Frazzetto, 2022). With the help of AI, compliance alerts could be more accurately filtered, minimizing the need for manual review by compliance officers and in that way effectively reducing overall compliance costs. Dzhaparov (2022) looks at the use of AI in the Private Wealth Management (PWM) industry to meet compliance regulations and improve efficiency and discusses the benefits of employing it. According to the author, one of the benefits is that NLP and Machine Learning (ML) enable a comprehensive and dynamic understanding of the requirements of PWM users. These advanced technologies allow for real-time data updates, facilitating a holistic perspective of the customer. Furthermore, the adoption of RPA proves highly valuable in mitigating compliance risks and minimizing associated costs by significantly reducing the resources required for manual monitoring of regulatory changes. Kaya et al., 2019) elaborate that RPA software eliminates reliance on human involvement in repetitive tasks, allowing employees to allocate their efforts toward core business objectives and operations. Implementing RPA according to the research can lead to significant cost savings ranging from 25% to 50%. Compared to employing a full-time offshore employee, the cost of a software robot is approximately one-third, making it a cost-effective solution. Han et al. (2020) provide an overview of the current academic research on the application of AI in the field of AML. The authors introduce a novel framework that leverages advanced techniques in natural language processing and deep learning. They describe one feature – Entity Recognition (ER), which is essentially a collection of algorithms that possess the ability to identify and extract important entities, for instance, individuals or job titles from a given input text, which enables accurately

analyzing textual data in a more efficient matter. Furthermore, the research proposes the utilization of sentiment analysis to significantly expedite the investigation process for compliance officers. Authors elaborate that this technique could be applied across various stages, for example, backlog management, and customer onboarding process, where the purpose of operations is identifying significant sentiment patterns and trends associated with individual customers. According to the research, the proposed framework was applied in the practice – feedback received from end users suggests that there is a positive outlook on the potential reduction of time spent investigating red-alerted transactions by 30%.

Pontes et al. (2022) look at anti-money laundering procedures in the United Kingdom. The authors identify several problems that have an impact on cost increase in AML. Based on research, regulatory bodies maintain their emphasis on traditional controls and offer limited support or incentives for financial institutions to foster innovation or develop risk-based solutions. The absence of a clear stance from regulatory supervisors on the permissibility of replacing outdated techniques results in financial institutions investing substantial resources in ineffective controls. Furthermore, the study shows that law enforcement agencies do not provide enough guidance for financial institutions when filing reports. Only a fraction of 3% of suspicious activity reports submitted to the financial intelligence units prove immediately useful for investigative purposes, indicating that a significant amount of 97% of the effort exerted by financial institutions in producing these reports is unlikely to result in any enforcement action.

Ciancimino (2023) suggests a few ways businesses could reduce their compliance costs while remaining compliant. The first strategy is to automatize the process as much as possible. The article elaborates that the market is witnessing a significant surge in the adoption of automated platforms that facilitate the centralization of diverse governance, risk management, and compliance (GRC) initiatives, resulting in potential benefits. IBM (n.d.) describes GRC as an organizational strategy to manage governance, risk management, and compliance within an organization while adhering to industry and government regulations. It involves a suite of software capabilities that facilitate the implementation and management of an enterprise GRC program. According to IBM (n.d.), by employing the GRC model companies can effectively address IT and security risks, reduce operational costs, and ensure compliance with relevant regulations. Furthermore, GRC provides an integrated perspective on risk management, which aids in better decision-making and overall better performance of a company. Handoko et al.,

(2020) conducted qualitative research, which involved gathering primary data through informant interviews, complemented by the utilization of secondary data from already published research papers and reports that pertain to GRC. The findings indicate that successful indication of GRC within a company yields several significant outcomes, such as the ability to anticipate and analyze potential risks that may arise in the future. Al Habsyi et al. (2021) conducted an empirical analysis of 30 companies that won the Top GRC Award in 2019 and 2020. By employing quantitative analysis (SPSS for multiple linear regression analysis) authors of the research portray that GRC and intellectual capital show a positive effect on the company's performance level. Findings show that the combined influence of governance, risk, and compliance variables along with intellectual capital accounts for 50.7% of the company's performance.

Revisiting an article by Ciancimino (2023) another strategy to reduce compliance costs in the long run is to invest in compliance resources and personnel. According to the article, maximizing return on investment (ROI) in terms of compliance costs is achieved through the establishment of dedicated internal resources that possess a comprehensive understanding of contractual obligations, regulatory mandates, and commitment to safeguarding customer data. Furthermore, the author stresses the fact that while the recruitment of a compliance officer may involve substantial costs, the consequences of non-compliance far outweigh the expenses associated with maintaining compliance. It is worth noting that on average the financial repercussions of non-compliance are 2.65 times higher compared to the costs incurred in ensuring adherence to regulatory requirements. Furthermore, investing in cybersecurity is a significant financial commitment for organizations in terms of compliance. (Lee, 2021) describes that in the contemporary business landscape, cybersecurity holds a prominent position as a crucial element within the framework of enterprise risk management. The escalating frequency of cyber breaches has led to severe and consequential damages affecting both organizations and individuals. These damages encompass various detrimental consequences, including breaches of compliance obligations.

Overall, the adoption of AI, RPA, and NLP emerges as a promising avenue to enhance operational efficiencies and mitigate costs associated with regulatory compliance.

In summary, this review delves into the multifaceted landscapes of anti-money laundering and data protection, emphasizing the pronounced financial implications

accompanying regulatory compliance. The exploration of anti-money laundering-related literature reveals escalating costs, particularly burdening larger institutions, driven by regulatory expansions. The confluence of AML and data protection costs highlights the economic challenges inherent in regulatory compliance, underscoring the need for careful resource allocation and the adoption of innovative solutions to fortify organizations against evolving regulatory landscapes. Amid these challenges, technological interventions, such as AI and RPA, emerge as strategic avenues offering not only operational efficiencies but also substantive reductions in compliance expenditures.

In essence, this comprehensive analysis underscores the intricate relationship between regulatory demands and organizational costs. It emphasizes the inevitability of costs while advocating for a balanced approach that navigates the regulatory complexities and optimizes resource allocation, fostering a resilient and cost-effective future.

2. METHODOLOGY

In the empirical part of this thesis to investigate the costs of anti-money laundering and data protection for companies and in addition explore the possible ways for a reduction of said costs, an extensive survey was conducted.

To start, this thesis explores a critical problem centering around the financial and operational burdens associated with anti-money laundering compliance and data protection measures. The **problem** this thesis investigates is the magnitude of financial resources firms allocate to anti-money laundering and data protection measures, the challenges firms face in managing and mitigating these costs as well as the opportunities and strategies available to firms for reducing anti-money laundering and data protection costs while maintaining compliance. Furthermore, this thesis investigates how certain variables – asset size, industry, and others make an impact to the extent of how much companies spend on being compliant with regulations related to anti-money laundering and data protection.

The main hypotheses to be tested by this research:

H1: There is a significant linear relationship between the size of a company (measured by asset size) and its anti-money laundering compliance costs and/or data protection costs.

The hypothesis examines whether larger companies tend to experience proportionally higher anti-money laundering compliance costs. The main goal of this hypothesis is to uncover whether the effort and resources invested in compliance scale up as companies grow.

H2: Companies with higher awareness and/or regulatory requirements as well as investments related to anti-money laundering/data protection initiatives experience higher AML/data protection costs.

The hypothesis aims to examine whether there is a positive correlation between regulatory awareness and financial commitment to robust AML compliance. Furthermore, it aims to investigate if strategic investments in data protection contribute to increased expenditures.

H3: Data protection costs are positively correlated with anti-money laundering costs, indicating synergy and interdependence between efforts to combat financial crime and data protection initiatives.

The empirical part of the thesis is divided into two parts – the qualitative phase and the quantitative phase. The mixed methods are being applied to gain the most comprehensive understanding of the problem.

2.1. Survey Methodology and Data Collection

In the first part of the empirical part of the thesis – phase 1, an extensive survey is employed to collect data from companies across various industries and countries. The survey consisted of four parts – general information about the company, anti-money laundering compliance, data protection compliance, and additional commentary the participant of the survey may want to provide.

In the first part of the survey, **general information** about the company was collected. To start, participants were asked to provide the primary location of the company to understand the geographical distribution of surveyed companies.

The next question aimed to categorize companies by industry sectors allowing for the analysis of the specific sectors. The sectors were selected based on NACE codes. According to Eurostat (2023), NACE, short for North American Industry Classification System is an acronym that is used to denote the different statistical classifications of economic activities that have been established in the European Union since 1970.

NACE classification serves as the structure element for the collection and representation of a wide selection of statistical information based on economic activities. This includes economic statistics such as business statistics, data on the labor market, national accounts along various other statistical domains. It can be compared at the European and world levels as well therefore it was selected to be used for this survey. The NACE framework's structure can be summarized as follows based on Eurostat (2023):

- The initial level comprises headings designated by alphabetical codes, denoted "sections".
- The second level involves headings represented by two-digit numerical codes, denoted as "divisions".
- The third level encompasses headings identified by three-digit numerical codes, denoted as "groups".
- The fourth level includes headings distinguished by four-digit numerical codes, labeled as "classes".

In a survey conducted by the thesis, the participants were asked to select the industry their company is operating in only by the first, initial level, selecting the suited "section" for the

most simplistic selection, and afterward, the participants had the option to specify the industry in an open-ended question. The industries from which participants could select were designed as follows (Table 1).

Table 1.

NACE Industry Sections

Section	Title
A	Agriculture, forestry and fishing
B	Mining and quarrying
C	Manufacturing
D	Electricity, Gas, Steam and Air Conditioning Supply
E	Water Supply, Sewerage, Waste Management and Remediation Activities
F	Construction
G	Wholesale and Retail Trade
H	Transporting and Storage
I	Accommodation and Food Service Activities
J	Information and Communication
K	Financial and Insurance Activities
L	Real Estate Activities
M	Professional, Scientific and Technical Activities
N	Administrative and Support Service Activities
O	Public Administration and Defence, Compulsory Social Security
P	Education
Q	Human Health and Social Work Activities
R	Arts, Entertainment and Recreation
S	Other Service Activities
T	Activities of Households as Employers
U	Activities of Extraterritorial Organisations and Bodies

Source: compiled by the author

Finally, the participants were asked to select the company's asset size based on the provided ranges. This question was used to gather information about the approximate scale of companies' assets. Asset size reflects industry norms and standards, which makes it easier to compare survey responses across different companies and industries. Furthermore, the selected ranges in the question covered a broad spectrum of company sizes, from small businesses to large corporations, ensuring that the survey captures a wide range of companies, making data more comprehensive. By providing already set, distinct categories with already defined thresholds respondents could easily identify, which range best represents the company's asset size.

The next part of the questionnaire consisted of questions related to **anti-money laundering compliance**. Participants were asked to specify whether their companies have specialized roles or departments responsible for anti-money laundering compliance. The follow-up question – determined the quantification of the financial resources a company allocated to anti-money laundering compliance efforts. Furthermore, participants of the survey were asked to rate their company's current anti-money laundering compliance efforts. This question aimed to assess the perceived effectiveness of the anti-money laundering compliance measures. The last two questions of the survey were related to assessing the knowledge of a company of anti-money laundering regulations specific to the companies' industries and the final open-ended question of this part of the survey allowed the respondents to provide qualitative insights into the challenges they encounter when dealing with anti-money laundering regulations.

The following part of the questionnaire was related to assessing the company's information regarding **data protection**. The first question of this part aimed to determine whether companies allocate their resources to data protection and cybersecurity. Next, respondents were asked to evaluate on a scale of 1 to 5, how their company is concerned about the data breaches and data protection costs. This question aimed to get insights into the relevance of the topic for the company and aimed to quantify companies' levels of concern regarding data breaches and related costs. Following that respondents were asked to choose the types of data protection measures they have implemented and quantify the financial resources allocated to data protection and cybersecurity efforts. Furthermore, open-ended questions invited participants of the questionnaire to provide details about any recent data breaches or security incidents that may have happened in the last two years. In addition, the survey collected data on whether companies were actively seeking cost-reduction opportunities in data protection. Finally, in the data protection part of the questionnaire, participants of the survey were asked open-ended questions, which allowed them to describe strategies and initiatives related to cost reduction in data protection.

The last part of the survey was voluntary – called **additional comments**. It was an open-ended question that allowed respondents to provide additional insights or comments on the topics of anti-money laundering compliance, and data protection costs and give additional thoughts regarding their company's approach to these topics under investigation.

The survey was conducted online, using web-based form software forms.google.com. The participants were selected by non-probability sampling method. According to McCombes (2023) using the non-probability sampling approach, individuals (in this thesis – companies) are chosen not based on a random selection. Thus, consequently, there is no equal opportunity for every individual to be included. According to the author, while the non-probability sampling method offers advantages in terms of accessibility and cost-effectiveness, this method heightens the risk of introducing sampling bias. Going further, quota sampling was employed in this thesis. According to McCombes (2023), this type of sampling involves a deliberate and non-random random selection of a fixed number proportion of units, known as quotas. The initial step entails categorizing the population into distinct and non-overlapping subgroups, referred to as strata, followed by the recruitment of sample units until the predetermined quota is met. These selected units share predefined characteristics, as determined by the researcher before the formation of strata. The primary objective of such sampling is to exercise control over the composition of the sample regarding specific attributes or traits. The 2 quotas used for the thesis were based on a country and industry. To start, the thesis selected respondents based on geographical region – Scandinavian countries (4 countries), Baltic Countries (3 countries), Central/Western European Countries (6 countries), and North America (1 country) (Table 2).

Table 2.

Country Selection

Scandinavian Countries	Baltic Countries	Western/Central Europe Countries	North America	Total
Finland	Lithuania	Poland	United States	
Norway	Latvia	France		
Sweden	Estonia	Germany		
Denmark		United Kingdom		
		The Netherlands		
		Spain		
4	**3**	**6**	**1**	**14**

Source: compiled by the author

Then looking at each geographical region, companies were selected based on industries selected by division on NACE codes (21 industries). 5 companies for each industry and each country were then selected at random, based on the availability of contact information. In this calculation, 1470 companies were contacted.

$$Surveys\ sent = 5\ * no.of\ NACE\ indutries * no.of\ countries \quad (1)$$

The contacts of the participants were found by going to public websites and using emails for general invoices or if relevant parties were specified in the company's webpage (e.g., employees working in the compliance sector) they were contacted directly. To ensure the confidentiality of the survey, the participants were informed beforehand that all information provided will be kept strictly confidential and will only be used for academic purposes and academic research. Furthermore, the questionnaire was designed in such a way as to avoid any parts that could help detect specific companies based on its answers. Based on the sensitive nature of the topic (company's expenses and disclosure of internal policies) companies did not have to include the company's name anywhere only the industry and the primary location of the country solely for sampling and further investigation and comparisons.

2.2 Models for AML and Data Protection Costs

In the second phase of the empirical part of this thesis, a quantitative approach is employed. Analyzing survey data using quantitative methods offers a systematic and unbiased approach to interpretation. By employing statistical techniques, one can arrive at robust conclusions, minimizing the influence of personal biases and ensuring a more objective evaluation of the data.

To explore potential causal relationships between different variables the multiple linear regression analysis was employed. According to Soetewey (2021), multiple linear regression is used to evaluate the relationship between two variables, however considering the effect the other variables cause as well. According to Soetewey (2021), guidelines for multiple regression analysis, several assumptions must be satisfied:

1. Linearity of relationships
    a. The relationship between dependent and independent variables should be linear.
2. Observations must be independent of each other.
3. The residuals, or the differences between observed and predicted values should follow a normal distribution.
4. Homoskedasticity of residuals

   a. The variance of the residuals should remain constant across all levels of the independent variables.
5. Absence of influential points (outliers)
   a. There should be no influential data points that could impact the model.

Additionally, Soetewey (2021), emphasizes the importance of addressing multicollinearity in multiple linear regression. Multicollinearity arises when there is a substantial linear correlation between independent variables, given the other variables in the model. This condition can lead to imprecise or unstable parameter estimates when there are changes in the variables. Strategies to mitigate multicollinearity include removing correlated independent variables or standardizing the data.

The first model in the empirical part of this thesis aimed to evaluate the relationship between anti-money laundering costs and other variables such as asset size, data protection costs, anti-money laundering efforts, and regions and industry variables. Thus, the first model was determined as follows:

$$AMLCosts_n = \beta_0 + \beta_1 AssetSize_n + \beta_2 AMLOF_n + \beta_3 AMLEF_n + \beta_4 AW_n + \beta_5 DPInv_n + \beta_6 DPEF_n + \beta_7 DPCosts_n + \sum_{i=1}^{k} \beta_{region_i} D_{Region_i} + \sum_{j=1}^{m} \beta_{Industry_j} D_{Industry_j} + \epsilon \quad (2)$$

where:

- $AMLCosts_n$ – compliance costs of a company
- β_0 – intercept
- $AssetSize_n$–asset size of a company
- $AMLOF_n$ – binary variable portraying if the company has a dedicated AML compliance department or officer
- $AMLEF_n$ – ordinal variable taking values from 1 to 5 measuring company's current anti-money laundering compliance efforts
- AW_n – binary variable measuring awareness of the regulatory requirements related to anti-money laundering
- $DPInv_n$ – binary variable portraying if the company invests in data protection and cybersecurity measures

- $DPEF_n$ – ordinal variable taking values from 1 to 5 measuring company's concerns about data breaches and data protection costs
- $\beta_7 DPCosts_n$ – data protection costs of a company
- $\sum_{i=1}^{k} \beta_{region_i} D_{Region_i}$ – the sum over *k* regions as dummy variables, where D_{Region_i} is *ith* region dummy variable
- $\sum_{j=1}^{m} \beta_{Industry_j} D_{Industry_j}$ – the sum over m industries as dummy variables, where $D_{Industry_j}$ is *jth* industry dummy variable
- ϵ – random error term
- n = 54 surveys
- k = 4 regions
- m = 19 industries

The second model employed in the empirical part of this thesis aimed to evaluate the relationship between data protection costs and other variables such as anti-money laundering costs, asset size, anti-money laundering efforts, and regions and industry variables. Then, the second model was estimated as follows:

$$DPCosts_n = \beta_0 + \beta_1 AssetSize_n + \beta_2 AMLOF_n + \beta_3 AMLEF_n + \beta_4 AW_n + \beta_5 DPInv_n + \beta_6 DPEF_n + \beta_7 AMLCosts_n + \sum_{i=1}^{k} \beta_{region_i} D_{Region_i} + \sum_{j=1}^{m} \beta_{Industry_j} D_{Industry_j} + \epsilon \quad (3)$$

In the second model estimated in the empirical part of this thesis, all the variables employed have the same meaning as in the first model.

In the questionnaire, there were a few categorical variables, where respondents were asked to select the appropriate range that best describes the asset size of the company. Furthermore, they were asked to select a range of approximate anti-money laundering and data protection costs that best described the situation in their company. In the subsequent regression models, the specific numerical values were chosen for independent variables $DPCosts_n$, $AMLCosts_n$ and $AssetSize_n$ based on the ranges of the questions. Ordinal coding was used as these numerical values were assigned as the midpoints of their respective categorical ranges.

Furthermore, to account for region and industry dummy variables were chosen. Each dummy variable corresponds to a specific region and specific industry dummy variables for industries were selected. This allowed the models to account for the variation in the dependent variable associated with different regions and industries since they are non-numeric. To avoid multicollinearity industry S – Other Service Activities industry and North America region were omitted.

To cater for the linearity of relationship conditions, correlation matrix was estimated to look for strong linear conditions.

Having ensured that the multiple regression conditions are satisfied, models for anti-money laundering and data protection costs were estimated using spreadsheet editor Microsoft Excel, where Excel add-in *RegressIt* was employed, which performs multivariate descriptive data analysis.

3. ANALYSIS OF THE RESULTS

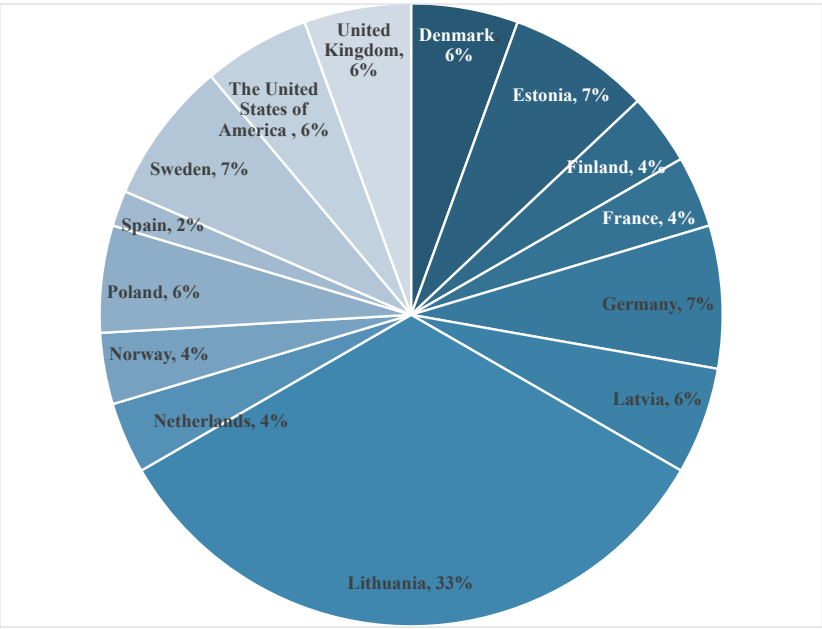
3.1.Questionnaire survey demographics

This section of the thesis is devoted to the quantitative analysis and discussion of the results obtained from the questionnaire survey.

To start, a total of 54 respondents participated in the online survey from the 1470 companies that were contacted. The response rate of the survey therefore is 3.67%. This result is relatively low and can be attributed to various factors. First, survey fatigue – companies, especially larger ones often receive numerous survey requests, which can lead to companies being less inclined to participate. Furthermore, the method of the survey can impact the response rate – since companies were contacted via email, they could end up in spam folders and be easily overlooked, while other methods like phone surveys or in-person interviews may yield different results. The second reason is the nature of the questions – the survey concerns sensitive topics (costs of the companies) therefore it could lead to resistance in participation even though the respondents were informed that the survey is anonymous and nowhere in the survey company can be identified.

Figure 2

Country distribution of respondents in a survey, N=54



Source: compiled by the author

Overall, there were companies from 14 countries that participated in the survey. The largest part of respondents was from Lithuania (33%), while the smallest percentage of respondents came from Spain (2%) (Figure 2). It is important to mention the largest portion of respondents came from Lithuania – it correlates with the fact that while conducting the survey author of the thesis had a greater accessibility of contacts with larger probability of receiving answers from the companies, while still maintaining quota sampling rules (5 companies per industry).

Furthermore, countries were separated by regions (Table 2), where Baltic countries composed 46% of all respondents, Scandinavian countries – 20%, western/central Europe countries – 28%, while North America made up 6% of the whole distribution.

Going further, the breakdown of respondents' reported industries is portrayed in Table 3.

Table 3.

Breakdown of reported industries, N=54

Industry:	Percentage of respondents:
A - Agriculture, forestry and fishing	4%
B - Mining and quarrying	2%
C - Manufacturing	4%
D - Electricity, gas, steam and air conditioning supply	4%
E - Water supply; sewerage; waste managment and remediation activities	2%
F - Construction	6%
G - Wholesale and retail trade; repair of motor vehicles and motorcycles	7%
H - Transporting and storage	4%
I - Accommodation and food service activities	2%
J - Information and communication	11%
K - Financial and insurance activities	28%
L - Real estate activities	6%
M - Professional, scientific and technical activities	4%
N - Administrative and support service activities	4%
Other (please specify in the next question)	2%
P - Education	4%
Q - Human health and social work activities	4%
R - Arts, entertainment and recreation	4%
S - Other services activities	2%
Grand Total:	**100%**

Source: compiled by the author

The survey answers based on quota sampling encompass a wide array of industries, ranging from agriculture, mining, and manufacturing to information and communication, financial services, and more. Notably, the financial and insurance sector (NACE code K) represents the largest proportion of respondents at 28%. This suggests a significant representation of this sector in the study. It also suggests that companies in the financial and insurance activities sector have a strong interest in anti-money laundering and data protection compliance. Given the nature of their operations and the sensitivity of financial data, their high participation is expected. The information and communication sector (NACE code J) is the second most represented sector with 11% of respondents. This sector's prominence may indicate its relevance in the research. It indicates that companies in this sector recognize the importance of anti-money laundering and data protection measures, possibly due to handling sensitive customer data and communication systems. Furthermore, several sectors, such as construction, wholesale and retail trade, and real estate activities have relatively balanced proportions of respondents, each accounting for 6-7% of the total. This may suggest that anti-money laundering and data protection requirements are relevant across various sectors. In addition, it might indicate that these industries are actively addressing compliance needs, possibly due to legal and regulatory obligations. Sectors like mining and quarrying, water supply and waste management, and accommodation and food services have comparatively lower representation, each accounting for 2% of respondents. It may indicate that these sectors might perceive anti-money laundering and data protection as less applicable or have lower regulatory requirements in these areas thus the lower participation rate from companies operating in these sectors.

Furthermore, it is important to mention that there were no respondents from 3 industries:

- O – Public Administration and Defense; compulsory social security.
- T – Activities of households as employers; undifferentiated goods – and services – producing activities of households for own use.
- U – activities of extraterritorial organizations and bodies.

The companies from these sectors might have not responded to the questionnaire for several reasons. To start, the content and subject matter of this survey may not be relevant for these sectors. Public administration, defense, household activities, and extraterritorial organizations

have distinct functions that may not directly correlate with the concerns addressed in surveys related to anti-money laundering and data protection in the private sector. Furthermore, sectors such as public administration and defense are often subject to their specific regulatory frameworks, which may not be regulated by the same regulatory bodies as in the private sector, which can result in a lack of engagement. Moreover, these sectors (public administration and defense) frequently manage and operate with sensitive and classified data – the unique status of such companies raises more concerns about the confidentiality of the survey. Furthermore, it is important to mention that companies in section T (activities as households) are primarily oriented towards personal instead of non-commercial pursuits. Therefore, their activities may not involve the same financial transactions and data processing, which would be typical in the private sector, thus decreasing the relevance of this questionnaire for this segment of companies.

3.2.Quantitative Approach Results

This subsection is dedicated to presenting and discussing the findings of quantitative analysis of survey results. To start, to predict the dependent variable – anti-money laundering costs and identify the relationship between the dependent variable and other variables, such as asset size, data protection costs, anti-money laundering efforts, and regions and industry variables multiple regression was estimated. The findings can be found in Table 4.

The model's explanatory value is reflected by r-squared value – 0.839, which indicates a substantial proportion of variability in anti-money laundering costs is accounted for by the included variables since the model explains approximately 83.9% of the variability in the anti-money laundering costs. Root mean square error measures the average difference between predicted values of a statistical model and an actual model and is the standard deviation of the residuals. Root mean square error shows the distance between the regression line and the data points. (Frost, n.d.-b) In the estimated model root mean squared error was valued at 17,180 meaning that the predictions of a model deviated from the observed values by approximately 17,180 units. Root mean square error of such value in this model offers insights into the average magnitude of prediction errors.

Furthermore, while model fit and performance metrics suggest a decent fit of the model, it is important to consider the p-values. The majority of the variables have significantly large p-

values in the models, meaning that coefficients in the model do not demonstrate statistically significant associations with anti-money laundering costs. To better understand these relationships, additional investigation and potential adjustments to the model are needed for a more accurate analysis.

Looking at the variables in more detail, the coefficient of asset size is estimated at 0.000053, which indicates the estimated change in anti-money laundering costs for a one-unit increase in asset size. A positive coefficient indicates a positive relationship between asset size and costs spent on anti-money laundering.

Table 4.

Multiple Regression results, AML Costs

Variable	Coefficient	Std. Error	t-Statistic	P-value
Constant	-19,480	43,778	-0.445	0.660
A - Agriculture forestry and fishing	8,957	36,239	0.247	0.807
AMLEF	4,339	5,163	0.840	0.409
AMLOF	6,181	14,991	0.412	0.684
AW	12,413	12,967	0.957	0.348
AssetSize	0.000053	0.000098	0.543	0.592
B - Mining and quarrying	-28,229	42,834	-0.659	0.516
Baltic Countries	-5,594	18,555	-0.301	0.766
C - Manufacturing	423.175	37,221	0.011	0.991
D - Electricity gas steam and air conditioning supply	-30,812	34,326	-0.898	0.378
DPCosts	0.703	0.199	3.539	0.002
DPEF	4,699	4,600	1.021	0.317
E - Water supply sewerage waste management and remediation activities	-18,702	39,797	-0.470	0.642
F - Construction	4,158	34,455	0.121	0.905
G - Wholesale and retail trade repair of motor vehicles and motorcycles	13,277	32,505	0.408	0.686
H - Transporting and storage	-4,658	35,853	-0.130	0.898
I - Accommodation and food service activities	8,069	42,778	0.189	0.852
DPInv	-4,386	13,912	-0.315	0.755
J - Information and communication	-16,761	29,770	-0.563	0.578
K - Financial and insurance activities	6,208	28,558	0.217	0.830
L - Real estate activities	8,329	34,745	0.240	0.813
M - Professional scientific and technical activities	-17,770	33,586	-0.529	0.601
N - Administrative and support service activities	-23,016	34,461	-0.668	0.510
Other industry	-12,383	37,148	-0.333	0.742
P - Education	5,972	35,935	0.166	0.869
Q - Human health and social work activities	-8,753	38,160	-0.229	0.820
R - Arts entertainment and recreation	4,149	37,539	0.111	0.913
Scandinavian Countries	-4,872	15,278	-0.319	0.752
Western/Central Europe Countries	-12,787	15,570	-0.821	0.419
Base Region dummy - North America				
Base Industry dummy - S				
No.of observations = 54				
R-squared = 0.839				

Source: own calculations

Furthermore, the coefficient of data protection costs denotes that a unit increase in data protection costs is associated with a 0.703 unit increase in anti-money laundering costs. This variable also portrays a conventional significance level with a p-value of 0.002. Anti-money laundering efforts variable is estimated at 4.339, meaning that for each one-unit increase in this ordinal variable taking values from 1 to 5, there is an associated increase in anti-money laundering costs by 4,339 units. In addition, companies that have a dedicated anti-money laundering compliance department or officer are associated with higher anti-money laundering costs by 6,181 units compared to companies without a dedicated anti-money laundering compliance department or an officer (where $AMLOF = 0$). Furthermore, companies with higher awareness or regulatory requirements related to anti-money laundering are associated with higher anti-money laundering costs by 12,413 units compared to companies with lower awareness.

The ordinal variable *DPEF,* representing a company's concerns about data breaches and data protection costs exhibits a positive association with anti-money laundering costs. For each one-unit increase in *DPEF*, which ranges from 1 to 5, there is an estimated increase of 4,699 units in anti-money laundering costs. The binary variable *DPInv,* indicating whether a company invests in data protection and cybersecurity measures, demonstrates a negative association with anti-money laundering costs. Companies investing in data protection are associated with lower anti-money laundering costs by 4,386 nits compared to companies not making such investments. This could imply that proactive investments in data protection may contribute to cost reduction when looking at anti-money laundering costs.

When looking at coefficients of dummy industry variables industries such as electricity, gas, steam and air conditioning supply, mining and quarrying, and administrative and support service activities demonstrate negative coefficients (-30,812, -28,229, and -23,016 respectively), which would suggest lower anti-money laundering compliance costs. Such industries with negative coefficients are operating in a way where inherent exposure to money laundering risks is relatively low. However, according to the literature situation in the mining and quarrying sector is the opposite. According to Randhawa et al. (2022), the mining and quarrying industry is known as susceptible to bribery and corruption, because of intricate supply chains, which span various third-party entities across diverse and often high-risk jurisdictions. Furthermore, the manufacturing industry estimated coefficient at 423,175 proposes an increase in anti-money laundering costs compared to the omitted category. While

a p-value of 0.9911 indicates that the result is not statistically significant and the wide confidence interval (-76,235 to 77,082) further emphasizes the uncertainty in the estimated effect, the literature provides various reasons to support such a result. The manufacturing industry remains susceptible to significant risks of economic crime. According to the recent global study on occupational fraud conducted by the Association of Certified Fraud Examiners, the manufacturing sector ranked the second highest in the reported cases, where average losses amounted to US$240,000. In addition, many of the businesses in this sector face exposure to economic crime risks, which include bribery, corruption, breaches of economic sanctions, violations of export controls, and facilitation of tax evasion (Smith & Boddy, 2020).

Region dummy variables when compared to the North American region provided lower anti-money laundering costs. The western and central European countries indicated a decrease in anti-money laundering costs by 12,787 units, Baltic Countries by 5,594 units, and Scandinavian by 4,872. Negative coefficients may suggest that companies operating in these regions experience a more efficient regulatory environment. This could be because of the regulatory framework's effectiveness and government policies. Looking at the study conducted by Truskauskas & Taujanskaitė, (2022) cluster analysis results indicate that Baltic countries emerge as the most efficient in managing anti-money laundering practices. However, the interpretation suggests a potential controversy in the findings. The authors propose an explanation for the observed differences, proposing that Scandinavian countries may invest heavily in anti-money laundering measures, leading to the detection of more money laundering activities. In contrast, Baltic countries, while showing lower detection rates, might be interpreted as diligently working on the prevention of money laundering, despite lower investment levels (Truskauskas & Taujanskaitė, 2022)

According to Bortolotti (2018) representing each raw variable by a group of dummies results in a loss of one degree of freedom in the analysis. The number of degrees of freedom signifies the independent items of information available to estimate another item, and as the model becomes more precise, more degrees of freedom are sacrificed. Furthermore, another problem that can arise when using a lot of dummy variables is overfitting. According to Frost (n.d.), the problem of overfitting arises when one tries to estimate too many parameters from the sample. Estimating too many parameters from a sample can lead to issues, as each term in the model necessitates the estimation of a parameter using a fixed sample size. According to the author, it is recommended to have at least 10-15 observations for each term to ensure

trustworthy results (Frost, n.d.-a) To account for these problems and achieve more accurate and more statistically significant results of the model all the dummy variables were omitted from the regression. Thus, the results of modified multiple regression investigating anti-money laundering costs can be seen in Table 5.

Table 5.

Multiple Regression without dummy variables results, AML Costs

Variable	Coefficient	Std. Error	t-Statistic	P-value
Constant	-11,901	13,196	-0.902	0.372
AMLEF	2,568	3,728	0.689	0.494
AMLOF	7,545	9,505	0.794	0.431
AW	9,714	8,829	1.100	0.277
AssetSize	0.000086	0.000075	1.146	0.258
DPCosts	0.672	0.155	4.346	0.000
DPEF	2,376	3,164	0.751	0.456
DPInv	-8,949	9,787	-0.914	0.365
No.of observations = 54				
R-squared = 0.756				

Source: own calculations

The general summary of model fit provides moderately good results. The R-squared value of 0.756 indicates that approximately 75.6% of the variance in the dependent variable anti-money laundering costs can be explained by the independent variables in the model. Furthermore, the F-statistic tests the overall significance of the model, and in this case, with a p-value of 0.000, the model is statistically significant.

When looking at the coefficients for each independent variable the results are as follows. The anti-money laundering efforts rating variable indicates that a unit increase in the anti-money laundering efforts rating corresponds to an increase of 2,568 units in the estimated anti-money laundering costs. Furthermore, companies with anti-money officers (coded as 1) are estimated to have higher anti-money laundering costs by 7,545 units compared to those companies without anti-money laundering officers. These results coincide with the literature as well. According to the findings from a recent study on the true costs of financial crime compliance by (Forrester Consulting, 2023) 72% of respondents highlighted the escalating

salaries for full-time and part-time employees involved in financial crime compliance. Additionally, 71% of respondents reported increased technology costs as financial institutions transition to digital operations and remote work. Moreover, 69% of respondents cited a rise in compliance and know-your-customer software-related costs, underscoring the substantial expenses associated with the necessary technological investments to meet stringent compliance requirements. The study also identified outsourcing with a 69% increase and employee training costs with a 69% increase as well as significant contributors, emphasizing the considerable financial implication of building in-house expertise in the field of financial crime compliance. Looking further into regression results companies that are aware of anti-money laundering regulations have associated a 9,714 unit increase in the estimated anti-money laundering costs. This observed positive association indicates that companies with a demonstrated awareness of anti-money laundering regulations tend to incur higher costs, which would imply the correlation between regulatory awareness and the financial commitment to robust anti-money laundering compliance measures.

Furthermore, the asset size coefficient is estimated at 0.000086, meaning that for every unit of growth in asset size (for every euro), there is an associated rise of the value of the coefficient in the estimated anti-money laundering cost variable. The coefficient is relatively low due to the nature of the variable – asset sizes vary from 1M to 300M euros. The finding implies a positive correlation, suggesting that larger companies tend to incur higher anti-money laundering costs. This observed relationship emphasizes the potential impact of a business's scale on the financial commitment required for effective anti-money laundering compliance. Larger companies usually operate in larger multiple jurisdictions and are subject to more underlying regulatory requirements overall, as a developed company, seeks to excel in various functional areas including anti-money laundering and data protection compliance. According to Onfido (2023), robust anti-money laundering screening and monitoring enhances the trustworthiness of financial institutions, gathering trust from customers, employees, and regulatory bodies. This trust not only facilitates the retention of organizations but also fosters long-term business growth. Importantly, adherence to anti-money laundering standards allows institutions to concentrate on core business operations instead of grappling with the aftermath of money laundering incidents and rebuilding customer trust.

When examining the relationship between data protection costs and the estimated anti-money laundering costs, a noteworthy pattern emerges. To be more specific, a one-unit increase

in data protection costs is correlated with the corresponding increase of 0.672 units in the estimated anti-money laundering costs. This result is supported by a p-value of 0.000 indicating a statistically significant result. This result suggests a positive association, indicating that higher expenses incurred in data protection align with heightened estimated costs in anti-money laundering measures. Similarly, the data protection efforts rating variable estimated a unit increase in the data protection efforts rating corresponds to an increase of 2,376 units in the estimated anti-money laundering costs. This implies the notion that more robust efforts and investments in data protection are correlated with higher estimates of anti-money laundering costs. Important to note that this result is similar to the anti-money laundering efforts variable, suggesting a parallel approach of the business, meaning that if the company tries being compliant with anti-money laundering compliance, the same could be said about the data protection. In contrast, the variable data protection investments provide an interesting dynamic. Companies investing in data protection, denoted by the value of 1, are estimated to experience a decrease of 8,949 units in anti-money laundering costs compared to the companies not making such investments. This implies a potential cost-saving effect associated with strategic investments in data protection measures. According to the report by LexisNexis Risk Solutions (2021) one of the factors that contributes to increasing anti-money laundering costs is the fact that financial institutions are reportedly spending over 20 hours on remediating standard risk customers, where 90% of these cases are proving to be false positives. These inefficiencies are influenced by various underlying factors, such as disparate data systems and the lack of a unified view of customer risk. Challenges arise from incomplete or outdated data, which affects the volume of alerts handled by financial crime teams and causes delays in an ongoing screening when customer data is missing and inaccurate. Important to mention that compliance teams often have limited control over this area, as responsibility for handling customer data typically lies in other departments (LexisNexis Risk Solutions, 2021) .This example and similar ones in the industry support the fact that investments in data protection strongly influence and help to reduce anti-money laundering costs.

Proceeding further with the empirical part of this research, to investigate the relationship between data protection costs and other variables, for instance, anti-money laundering costs, asset size, anti-money laundering efforts, and regions and industry variables the second model was estimated, where the dependent variable was selected as data protection costs. The estimated results are portrayed in Table 6.

Table 6.

Multiple Regression results, Data Protection Costs

Variable	Coefficient	Std. Error	t-Statistic	P-value
Constant	-9,221	36,053	-0.256	0.800
A - Agriculture forestry and fishing	1,003	29,801	0.034	0.973
AMLEF	3,580	4,240	0.844	0.407
AMLOF	6,438	12,288	0.524	0.605
AMLCosts	0.475	0.134	3.539	0.002
AW	-6,201	10,773	-0.576	0.570
AssetSize	0.000214	0.000068	3.126	0.004
B - Mining and quarrying	26,927	35,076	0.768	0.450
Baltic Countries	-637.105	15,267	-0.042	0.967
C - Manufacturing	8,402	30,526	0.275	0.785
D - Electricity gas steam and air conditioning supply	21,475	28,321	0.758	0.455
DPEF	583.829	3,854	0.151	0.881
E - Water supply sewerage waste management and remediation activities	24,744	32,457	0.762	0.453
F - Construction	6,327	28,280	0.224	0.825
G - Wholesale and retail trade repair of motor vehicles and motorcycles	-56.234	26,787	-0.002	0.998
H - Transporting and storage	-22,915	29,100	-0.787	0.438
I - Accommodation and food service activities	6,941	35,134	0.198	0.845
DPInv	-11,393	11,221	-1.015	0.320
J - Information and communication	19,385	24,299	0.798	0.433
K - Financial and insurance activities	5,704	23,451	0.243	0.810
L - Real estate activities	6,571	28,541	0.230	0.820
M - Professional scientific and technical activities	8,995	27,681	0.325	0.748
N - Administrative and support service activities	20,255	28,268	0.717	0.480
Other industry	12,374	30,479	0.406	0.688
P - Education	15,873	29,361	0.541	0.594
Q - Human health and social work activities	7,839	31,337	0.250	0.805
R - Arts entertainment and recreation	-8,357	30,795	-0.271	0.788
Scandinavian Countries	7,187	12,492	0.575	0.570
Western/Central Europe Countries	6,489	12,895	0.503	0.619
Base Region dummy - North America				
Base Industry dummy - S				
No.of observations = 54				
R-squared = 0.871				

Source: own calculations

To start, the R-squared value of 0.871 indicates a robust fit, portraying that 87,1% of the variability in data protection costs is explained by the model. The adjusted R-squared was estimated at 0.727 suggesting that the inclusion of predictors did not blow out the goodness of the fit out of the proportion. Furthermore, the mean error, root mean squared error (RMSE) and mean absolute error (MAE) (estimated at 0.000, 14.111, and 9,596 respectively) collectively indicate that the predictions of the model closely approximate the actual values.

When looking at the variable portraying anti-money laundering costs, the positive coefficient of 0.475 implies that an escalation in anti-money laundering costs is strongly associated with a corresponding increase in data protection costs. This result is backed up by a

p-value estimated at 0.002 implying statistical significance. The estimated results suggest a strong synergy and interdependence between efforts to combat financial crime and data protection initiatives. According to Lisanawati & Sadeghi (2019), the importance of data in anti-money laundering processes is underscored by its role in facilitating law enforcement efforts. The data should not pose a limitation but rather be viewed as a valuable resource for investigating the nature of the crime. Furthermore, the variable portraying asset size estimated a positive coefficient of 0.000214 with a 0.004 p-value. It indicates that larger asset-sized companies tend to spend more on data protection measures. This suggests that large companies are facing increased complexity and scale of data protection measured. According to Anant et al. (2020), a significant obstacle, especially for globally operating companies, lies in the diverse and inconsistent nature of regulations across jurisdictions and markets. To tackle this challenge and proactively address potential future regulations, numerous companies are adopting a systematic approach to compliance. This includes establishing specific roles and responsibilities for regulatory compliance within their organizations and implementing solutions designed to withstand future regulatory challenges.

In addition, the binary variable data protection investments portray that companies investing the data protection measures ($DPInv = 1$) experience a notable increase of 11,393 units in data protection costs compared to those businesses that are not investing ($DPInv = 0$). This also supports the fact that active investments in data protection technology and other solutions would yield cost-saving benefits for the companies in the long term. According to a study done by Centre for Information Policy Leadership (2023) surveyed companies that implemented data privacy management programs 81% of the companies identified avoiding scrutiny or fines, 75% avoiding damage to reputation and 67% - experiencing less serious and fewer reportable data breaches. Furthermore, categorical variable corresponding to data protection efforts rating taking values from 1 to 5 estimated with a significantly positive coefficient of 583.829 units signifies that a higher rating by respondents of the survey in data protection efforts corresponds to an increase in data protection costs. This indicates that companies that are more concerned regarding data breaches and security incidents are most probably allocating a greater number of resources and efforts to enhance their data protection posture, which incurs higher associated data protection costs.

Looking at the dummy variables portraying industries and regions in the second model the same base industry and region variables were selected as in the first models, where the

dependent variable was anti-money laundering costs. To start, the largest coefficients could be seen in mining and quarrying, water supply sewerage waste management and remediation activities as well as electricity gas steam and air conditioning supply and administrative and support service activities industries with coefficients of 26,927, 24,744, 21,475, and 20,255 respectively. Companies operating in mining and quarrying may deal with sensitive information, which would require comprehensive measures to protect data effectively. The mining sector encounters various challenges that encourage the integration of new technologies. Big data, propelled by the rapid advancements in information and communication technology, stands out as a promising technology capable of transforming the entire mining domain. However, despite multiple endeavors to implement big data in mining, persistent issues, particularly those related to big data management, continue to challenge the industry (Qi, 2020). Furthermore, the water supply sewerage waste management and remediation activities industry as well as the electricity gas steam, and air conditioning supply industry show a large increase in data protection costs, since dealing with public utility services such businesses are handling extensive customer data, which requires robust data protection measures. Furthermore, according to Radosavljevic (2021), utility companies frequently become targets of cyber-attacks due to the valuable nature of the information they collect, making it a lucrative commodity on illicit markets. In the event of a data breach, companies subject to certain requirements are obligated to promptly notify affected customers upon discovery of the breach or notification by the vendor. Furthermore, looking into the results of the information and communication industry, the statistical analysis revealed a noteworthy coefficient of 19,385 in the regression model. This coefficient signifies a considerable positive influence on data protection costs in contrast to the reference category. This observation implies that companies within the information and communication sector tend to increase expenditures on data protection. Various factors could explain such findings. To start, the information and communication sector is known for its heavy reliance on processes that are technology-driven and the industry that manages confidential data. Businesses in this sector may expedient increased costs in data protection due to the nature of their business, such as managing extensive customer data, ensuring compliance to privacy regulations, and making investments to avoid cybersecurity threats. For instance, according to the Telecom Review (2021) in recent years, there has been a significant increase in cyberattacks targeting the telecom industry. This trend is attributed to the industry's control over extensive and critical communication infrastructure. The telecom sector considers data as an asset, catering not only to its own needs but also to various potential value-added service providers. More specifically,

telecommunication companies generate diverse forms of data, including call detail data, network data, and customer data. These datasets encompass information about all calls made within the networks, the status of hardware and software components in the networks, and identification details of end-users (Telecom Review, 2021).

Industry G and H dummy variables (wholesale and retail trade; repair of motor vehicles and motorcycles and transporting and storage) obtained negative coefficients of -56,234 and -22,915 respectively indicating that companies in these industries have lower data protection costs on average compared to the baseline category. It is potentially since companies in these sectors handle less sensitive or smaller amounts of data when compared to the industries that portrayed positive coefficients. Furthermore, based on the nature of this business, companies might have fewer privacy concerns or regulatory requirements compared to industries with higher coefficients.

Additionally, it is important to analyze the results of region dummy variables. The dummy variable portraying Baltic countries estimated a significantly negative coefficient of -637.105. This indicates a negative impact on data protection costs compared to the reference region. Besides, such a large negative coefficient suggests that companies in Baltic Countries may on average incur lower data protection costs. This could be a result of multiple factors – since the baseline region was selected as North America, the comparative size of the companies is larger, which influences cost size as well. Smaller companies in the Baltic region, responding to the survey, might not exhibit the same level of concern or investment in data protection compliance, which contributes to lower associated costs. To account for and look for reasons of the significantly high p-values the general trends of the survey answers were observed by filtering out results based on a specific industry. In Baltic countries region p-value is high, estimated at 0.967, which could be since the sub-sample of Baltic countries have diverse and dispersed responses regarding data protection costs. On the contrary, Scandinavian, and Western/Central Europe regions could be seen with positive coefficients of 7,187 and 6,489 respectively. These results suggest a positive impact on the data protection costs relative to the reference region. In comparative analysis, looking at the general trends of the responses, data protection costs in Scandinavian and Western/Central European countries were observed to be considerably higher and less dispersed than those in Baltic countries. Specifically, from the results of the regression, the expenditure in Scandinavian countries and Western/Central Europe surpassed that of Baltic countries by 7.8 thousand euros and 7.1 thousand euros,

respectively. Several factors may contribute to those differences. The larger markets and more comprehensive regulatory frameworks in Scandinavian and Western/Central Europe regions could lead to increased emphasis on and investment in robust data protection measures. In addition, the participation of larger companies in these regions in the survey may contribute to the elevated costs, as larger businesses typically allocate more resources to ensure compliance and safeguard data breaches. These regional distinctions underscore the nuanced landscape of data protection expenditure, which is influenced by market size, regulatory environments, and the scale of the participating entities. Supporting analysis can be found in the literature. For instance, the paper by Koski & Valmari (2020) claims that the results derived from the paper's data analysis indicate that the profit margin trends with European data-intensive firms during the initial year of GDPR implementation lagged those observed among their counterparts in the United States. The authors of the paper performed empirical analysis, where empirical findings revealed a notable discrepancy, with the profit marking of European data-intensive firms experiencing an increase that was approximately 1.7 to 3.4 percentage points less than the profit margins observed among their data-intensive counterparts in the U.S. (Koski & Valmari, 2020). Scandinavian and Western/European regions, where positive and high data protection costs were observed, could be indicative of heightened regulations in their jurisdictions. This aligns with the noticeable patterns in profit margin developments noted in the research paper, suggesting that the regulatory landscape could contribute to variations in business expenditures related to data protection.

Going further with the empirical part of this thesis, the identical modifications to the model were completed. To account for overfitting, dummy variables for regions and industries were omitted from the regression. The modified model results in a search for a relationship with data protection costs can be seen in Table 7.

The multiple regression model with data protection costs as the dependent variable and dummy variables of industries and regions excluded demonstrates a meaningful explanatory capacity with a relatively high R-squared value estimated at 0.813. This suggests that a significant part of the variability in data protection costs is accounted for by the included independent variables in the model. The adjusted R-squared is 0.785, which suggests a good fit when considering the number of predictors in the model.

Table 7.

Multiple Regression without dummy variables results, Data Protection Costs

Variable	Coefficient	Std. Error	t-Statistic	P-value
Constant	-8,288	10,611	-0.781	0.439
AMLEF	1,621	2,997	0.541	0.591
AMLOF	2,670	7,668	0.348	0.729
AMLCosts	0.433	0.100	4.346	0.000
AW	3,015	7,162	0.421	0.676
AssetSize	0.000231	0.000051	4.533	0.000
DPEF	2,330	2,531	0.920	0.362
DPInv	-2,211	7,917	-0.279	0.781
No.of observations = 54				
R-squared = 0.813				

Source: own calculations

The anti-money laundering efforts variable suggests that a one-unit increase in anti-money laundering efforts is associated with an estimated increase of 1,621 units in data protection costs. A positive coefficient of this value indicates that higher efforts in anti-money laundering activities are related to higher data protection costs as well. Similarly, the binary variable anti-money laundering officer's coefficient portrays a positive coefficient of 2,670 as well. This coefficient indicates that when companies have anti-money laundering officers present, there is an estimated increase of 2,670 units in data protection costs, compared to the companies that have no anti-money laundering officers employed. This finding suggests that companies with dedicated anti-money laundering staff are likely to have more complex compliance programs and are therefore likely to spend more on data protection measures. In addition, anti-money laundering costs portray a statistically significant result of 0,433 with a 0 p-value. This result indicates that companies that have already invested in anti-money laundering compliance are likely to be more aware of the importance of data protection and are therefore more likely to make investments to mitigate the risks of data and security breaches. This reverts to the consensus detected in the literature. An article by van Egmond et al. (2021) discusses that banks, acting as financial system gatekeepers bear the responsibility of identifying unusual transactions. However, criminal transaction activities frequently disperse across various banks thus leading to the challenges in detection of such transactions. Effective detection of financial crimes hinges on collaboration across financial institutions and data sharing. Despite these imperatives, legal frameworks like GDPR and data protection laws,

coupled with privacy concerns, may impose constraints on unrestricted data sharing. Privacy–enhancing technologies emerge as promising solutions, facilitating collaboration without compromising the confidentiality of sensitive data (van Egmond et al., 2021). Going forward, the independent binary variable representing awareness of anti-money laundering measures indicates that when a business is aware of anti-money laundering requirements, there is a 3,015 increase in data protection costs, when compared to the companies not aware of such regulations. Companies that are aware of anti-money laundering compliance requirements in their jurisdiction are more likely to understand the risks associated with data breaches and non-compliance consequences. This could potentially lead to a greater willingness to invest in data protection measures to mitigate such risks that could arise. Furthermore, companies that answered "Yes" to the awareness question are more likely to operate in sectors, which focus more on compliance with such regulations, for instance, companies operating in financial or information and communication industries. Looking at the further results of this model, the independent variable representing asset size correlates with the initial model with dummy variables. A coefficient of 0,000231 suggests that larger companies tend to have higher data protection costs. The coefficient portrays statistical significance with a p-value of 0.000.

Independent variable, which rates the data protection rating of a company signifies that an incremental increase in the rating of data protection costs, measured on an ordinal scale taking values from 1 to 5 is linked to an estimated increase of 2,330 units in data protection costs. This indicates a positive correlation, implying that as companies rate their efforts higher safeguarding data, there is a corresponding elevation in the anticipated costs associated with maintaining robust data protection measures. Furthermore, the binary variable representing data protection investments suggests that companies investing in data protection (when the variable takes a value equal to 1) are estimated to have a decrease of 2,211 units in data protection costs compared to those companies that responded to the questionnaire as not investing (when variable takes value equal to 0). This shows a negative relationship, indicating that investments in data protection led to lower data protection costs. This is supported by research in the literature as well. A benchmark study of 53 multinational organizations in the United States independently conducted by Ponemon Institute LLC (2017) shows that organizations in the study experienced an average compliance cost of $5.47 million, representing a 43% increase from 2011 (when compared to 2017).

In contrast, the average cost for organizations facing non-compliance costs was $14.82 million, marking a 45% increase from 2011. The data illustrates that there are evident financial

implications for non-compliance. Furthermore, the study suggests that investing in the compliance activities outlined can prove advantageous in averting non-compliance-related problems such as business disruption, declines in productivity, fees, penalties, and other legal and non-legal settlement costs (Ponemon Institute LLC, 2017).

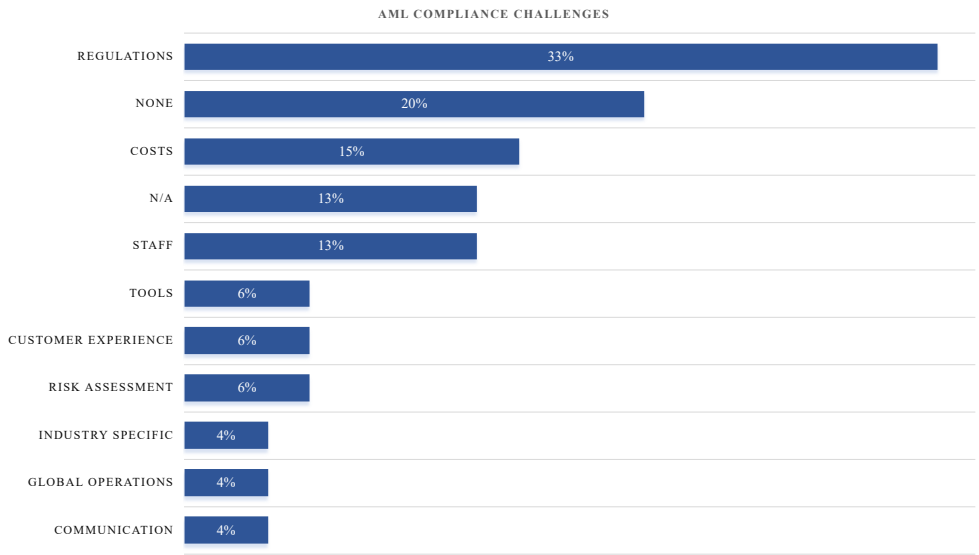
3.3.Qualitative Approach

In this subsection of the thesis, the remaining questions of the questionnaire will be analyzed, which were not included in the models discussed in section 3.3.

To start, the open-ended question "What challenges or obstacles does your company face when it comes to AML compliance?" aimed to understand and analyze the specific difficulties and barriers that a respondent company may encounter when ensuring compliance with anti-money laundering regulations. In the analysis of this question, each answer has been grouped into the categories seen in Figure 2. Since the same respondent could have enumerated different challenges, they were dispersed as the individual inputs to each category, hence the total percentage in the figure exceeds 100%.

Figure 3

AML Compliance Challenges



Source: compiled by the author

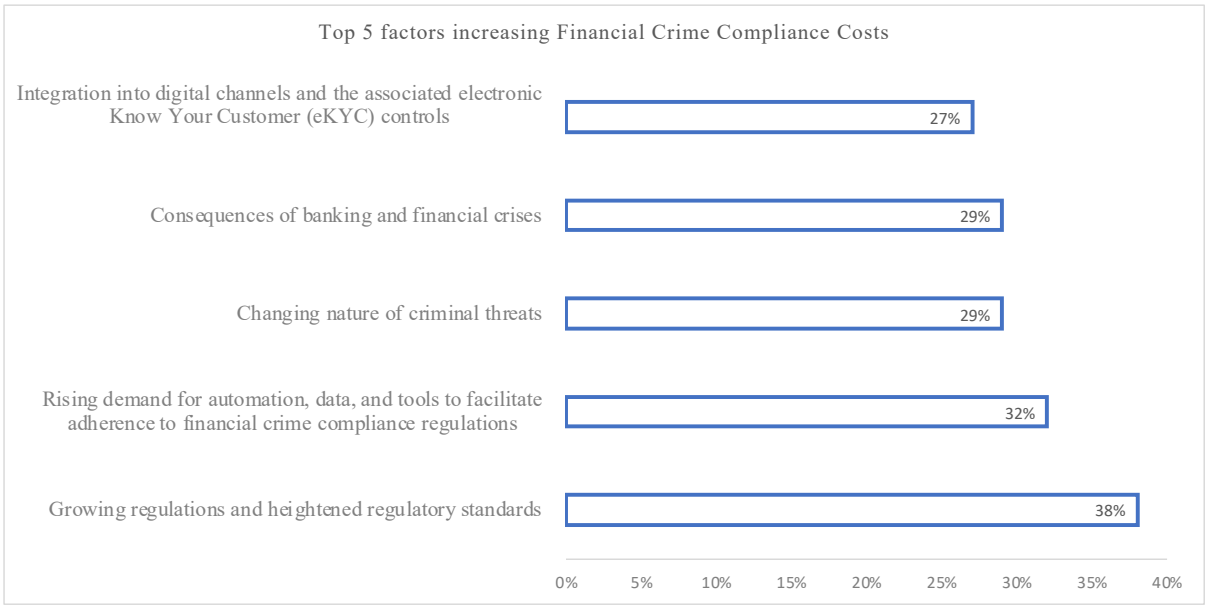
Looking at the results of this question, the largest percentage of respondents (33%) identified challenges related to anti-money laundering regulations. This indicates that a significant portion of respondents perceive compliance with regulatory requirements as a major obstacle. Looking at specific answers related to this one of the respondents specified that it is challenging “being compliant with always changing regulations”. For instance, the European Parliament has established the European Anti-Money Laundering Authority (AMLA) through regulation, conferring supervisory and investigative powers to ensure compliance with anti-money laundering and counter-terrorist financing requirements (European Parliament, 2023). This legislative measure reflects the ongoing commitment to enhance the regulatory framework for combating money laundering within the EU. However, such regulations unfortunately pose a significant impact to businesses. According to a FinTech Global (2023) survey, which encompassed over three thousand risk and compliance experts within the sector 72% of respondents in the European Union anticipate potential setbacks for their businesses due to new AML legislation, estimating costs between 360,000 euros and 1 million euros. The study further reveals that 97% of respondents foresee that a significant portion of these costs will likely arise from penalties, seizures, and escalation in training, monitoring, and reporting procedures (FinTech Global, 2023).

The 20% of survey respondents answered that they face no challenges in anti-money laundering compliance. Furthermore, another 13% of respondents answered that they were not sure or did not know of any challenges in the company – those were marked as N/A for simplicity purposes. Looking at the industries these respondents operate, most of those answers come from small companies operating in non-financial sectors. Such respondents who expressed uncertainty represent companies that are not fully aware of the challenges that could exist when dealing with AML compliance or have not yet encountered such issues. This also could relate that those are small companies that are mostly dealing with simple financial structures and transaction volumes, which leads to fewer or no anti-money laundering compliance issues. Furthermore, non-financial sectors also have different risk profiles when compared to financial institutions. In addition, looking at the specific answers of respondents, who answered as ‘none’ – some of the answers are from the larger companies – this could indicate that organizations have robust systems in place and could indicate a level of confidence in their compliance practices.

15% of respondents excluded costs as the biggest challenge they face when dealing with anti-money laundering compliance. This indicates that investing in anti-money laundering compliance measures poses a significant burden on organizations, which impacts budget allocation and distribution of the resources in the business. This reconciles with the literature and interconnects with the other challenges the respondents mentioned as the biggest challenges when dealing with AML compliance. A study by Forrester (2023) reveals that the primary driver is the burden of financial crime regulations followed by cost escalation due to the increased demand for advanced automation, intricate data analytics, and powerful tools, which emphasizes the evolving technological environment. Moreover, the study identified evolving criminal threats as a challenge, which showcases the increased sophistication of financial crime in the digital age as well as the consequences of the banking and financial crisis, which makes the industry more vulnerable. Finally, the study mentions the necessity for integration into digital tools and the implementation of comprehensive electronic Know Your Customer controls as one of the drivers for increased costs when dealing with financial crime compliance (Forrester Consulting, 2023). Figure 4 is compiled based on the results of the study by Forrester (2023) and portrays the distribution of study results.

Figure 4

Top 5 Drivers for Financial Crime Compliance Costs



Source: compiled based on Forrester Consulting on behalf of LexisNexis Risk Solutions (2023)

In addition, 13% of respondents in the survey mentioned staff as the highest-burden. More specifically, the respondent answers related to staff can be grouped into two largest challenges companies face – personnel and expertise and employee awareness and training. Personnel and expertise relate to respondent answers, such as “lack of personnel”, potential absence of “in-house experts” and “limited resources and staff expertise”, while employee awareness and training problem is based on answers such as “ensuring employees are well-informed about AML regulations and company-specific compliance policies” and “ensuring adequate training for staff”. These mentioned challenges by the respondents can contribute to increased costs for companies in several ways. To start, the recruitment process can induce costs – job postings, hiring recruiting agencies, extensive interview process, and onboarding. This correlates with the training expenses – investment in training programs to enhance the expertise of staff contributes greatly to the costs of the company, which could include purchasing training materials, hiring external trainers, and dedicating time for the employees to participate in the training, which would decrease the time spent on the operations in the production of the company.

Furthermore, 6% of participants in the survey singled out different kinds of struggles all of which in some way correlate with risk assessment, therefore those were grouped as well. One of the answers mentioned that. Determining and assessing the level of risk associated with different customers, transactions, and business relationships is a complex and time-consuming process. Such time-consuming risk assessment procedures can extend the operational business processes and transactions. Furthermore, a failed attempt to assess the needed risk level may result in inadequate anti-money laundering measures, which could expose the company to financial costs impacted by fines as well as losing customer trust and causing a loss in reputation. Another respondent mentioned cash transactions of the customers outside the normal channels, which poses a challenge. Monitoring and detecting cash transactions is crucial when complying with anti-money laundering regulations since failure to do this could potentially allow illicit funds to enter the financial system undetected. For instance, the operation led by French Customs authorities across 25 European Union member states revealed illicit movements of 18 million euros in cash, associated with money laundering, transactional criminal activities, and terrorism financing. Important to note that authorities identified 64 cases with potential linkages to money laundering, amounting to around 3 million euros and 20 cases potentially connected to sanctions against Russia for aggression against Ukraine, totaling approximately 180,000 euros (European Anti-Fraud Office, 2023).

Another 6% of respondents mentioned customer experience as a challenge they face when trying to comply with AML regulations. One answer stated that it poses a challenge "maintaining good customer experience while being compliant". It indicates recognition of a delicate balance that companies need to maintain between regulatory compliance and providing a satisfying experience for their customers. Since AML operations are quite complex, and often require rigorous customer due diligence, and monitoring of transactions, it could negatively impact customer satisfaction, since for instance, banks often present their customers with extensive onboarding processes (identity verification, and various documentation requirements). Furthermore, extensive transaction monitoring could delay or even cancel payments of the customers, which lessens trust and satisfaction, especially nowadays when customers increasingly expect seamless and swift interactions.

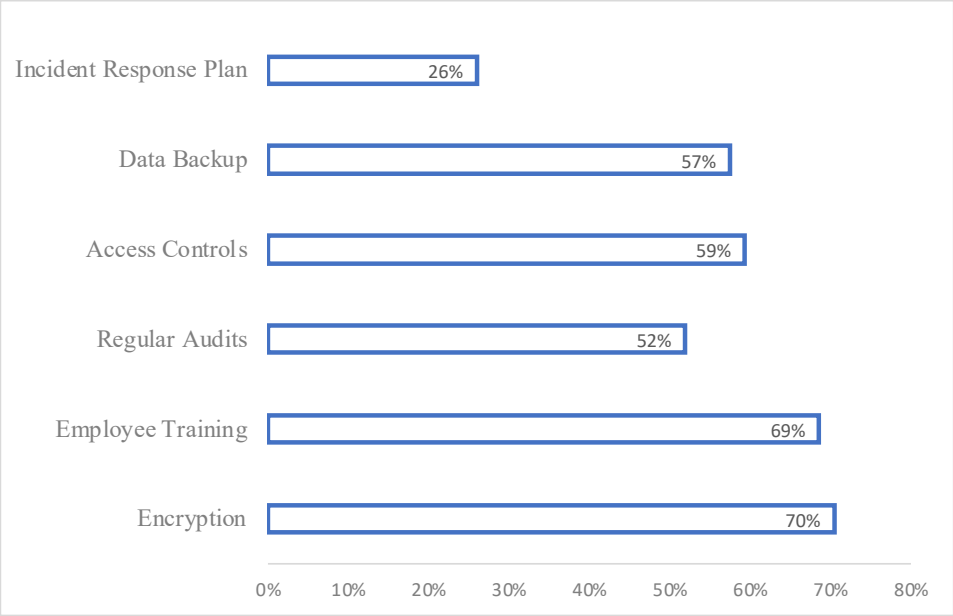
Other parts – tools, industry-specific, global operations, and communication were several entries with miscellaneous challenges mentioned. Looking at the tools as a challenge, a couple of respondents mentioned limited tools, or limited resources, which looking at those specific entries are small companies, most probably operating locally in non-financial sectors. On the contrary, few of the entries under global operations were larger companies that singled out difficulties when operating within the international market areas and complying with various jurisdictions.

In conclusion, the survey results highlight diverse challenges faced by businesses in the realm of AML compliance. The predominant concern is the evolving landscape of AML regulations, causing potential setbacks and financial burdens for a significant portion of respondents. The need to balance compliance with customer experience is evident, with complexities arising from stringent regulations and technological advancements. Overall, businesses navigate a complex landscape, requiring agility, technological adaptation, and strategic investments to address the multifaceted challenges caused by anti-money laundering regulations.

Progressing further with the qualitative stage of the thesis, a question in the survey "What types of data protection measures does your company currently employ?" is analyzed. The results of the distribution of the answers can be seen in Figure 5.

Figure 5

Data Protection Measures. N = 54



Source: compiled by the author

Overall, looking at the results of the distribution to this question – companies are most likely to use encryption and employee training as their data protection tools (70% and 69% respectively) followed closely by data backup and access controls with 57% and 59% of respondent answers respectively. This indicates quite a strong commitment to the foundational data protection measures in this sample of respondents. Companies employing encryption are most likely prioritizing data confidentiality, ensuring that if unauthorized access attempts succeed, the data will remain unreadable. Baig (2022) reported that according to an IBM study, the average cost of a data breach for organizations in 2021 was $4.24 and that the likelihood of a data breach is alarming with 30% of all businesses anticipated to experience such an incident. Also, the significance of data encryption in safeguarding businesses from breaches and mitigating severe financial and reputational consequences is emphasized (Baig, 2022). Furthermore, employee training is an essential part when building a strong culture of cybersecurity awareness. Educating employees on such topics reduces the risk of human errors happening when dealing with sensitive data. Privacy Engine (2023) highlighted several benefits of data protection training, including enhanced compliance with legal requirements, reduced risk of data breaches, improved reputation of a company, greater efficiency in handling data securely, and increased value for individuals through valuable skills and certifications (Privacy Engine, 2023). However, on the contrary, the Incident Response Plan was selected

only by 26% of respondents. The lower percentage suggests room for improvement in this area. Fairburn (n.d.) emphasized the critical need for organizations to have an Incident Response Plan to safeguard their data, and networks from malicious activities. This strategy enables quick detection and response to cyber threats, minimizing potential damage and ensuring the integrity of affected systems. Moreover, the presence of an incident response plan signifies the company's commitment to cybersecurity, acknowledging its potential impacts on employees, customers, and suppliers (Fairburn, n.d.). Thus, while the survey reveals commendable adherence to foundational data protection measures, there is an opportunity for companies to strengthen their resilience further by placing increased emphasis on the development and implementation of further tools and measures to avoid security incidents and protect their and customer's data.

In addition, respondents were asked if they had experienced any data breaches or security incidents in the past two years. Questions were open-ended asking respondents to describe the incidents if they answered positively. The results and the distribution of the received answers are portrayed in Table 8.

Table 8.

Data Breaches and Security Incidents in the past 2 years. Results distribution. N=54

Have you experienced any data breaches in the past two years?	Percentage	Have you experienced any security incidents in the past two years?	Percentage
None/Could not Disclose	80%	None/Could not Disclose	74%
Phishing	9%	Phishing	7%
Other Data Breaches	11%	Other Security Incidents	15%

Source: compiled by the author

The majority of respondents (80% and 74% for data breaches and security incidents respectively) reported experiencing no data breaches or security incidents in the past two years or could not disclose such information. This might indicate either effective data protection and security measures or hesitancy to disclose such incidents. Phishing being one of the most common cybersecurity threats was mentioned by 9% and 7% of the respondents in both categories – data breaches and security incidents. It correlated greatly with the literature as well. IBM Security's research revealed that in the study of 553 organizations, impacted by data breaches occurring between 2022-2023, the two most common initial attack vectors were

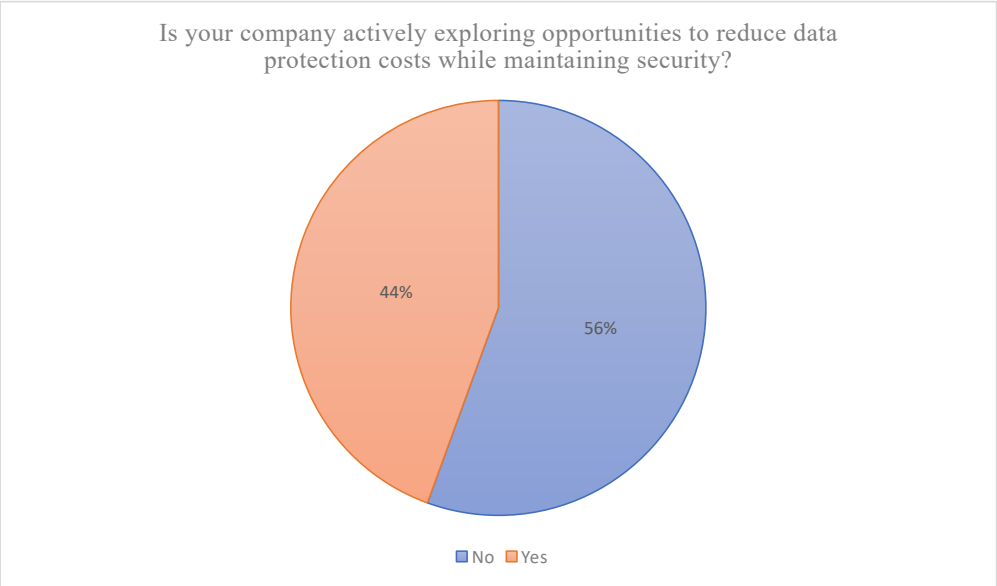
phishing and stolen and compromised credentials, accounting for 16% and 15% of breaches respectively. Furthermore, phishing, identified as the most prevalent attack vector, ranked as the second most expensive at $4.76 million (IBM Security, 2023).

Looking at other data breaches and security incidents in more detail, several different have been reported by the respondents. It involved incorrect customer contact when sensitive matters intended for one customer were mistakenly communicated to the wrong customer. Another respondent described an electronic invoice error, where 132 electronic invoices were exposed, which contained customer information, including names, addresses, and invoice numbers. Few answers mentioned attempted website and system intrusions, where companies faced multiple attempts to breach their websites and internal systems, highlighting the persistent threats of cyberattacks. One answer highlighted the importance of keeping up with the innovations, since due to having outdated software, one organization fell victim and patient records billing information, and critical medical systems were encrypted. In addition, there were several entries mentioning the importance of physical security as well, since few security incidents were mentioned such as missing key cards or work laptops being left in public places as well as individuals gaining unauthorized access credentials and keys to an office building of local office, which raises concerns regarding physical security.

Finally, the qualitative stage of this thesis delved deeper into the reduction of costs topic in the survey. The distribution of respondents when asked if they are considering cost reduction while remaining compliant can be seen in Figure 5. The distribution of responses suggests a quite even distribution, where a notable proportion of respondents see a value in actively exploring opportunities to optimize data protection costs. It could also indicate a broader trend within the business landscape where organizations are increasingly seeking ways to strike a balance between cost-effectiveness and robust security measures, reflecting the dynamic nature of the cybersecurity landscape and the need for strategic adaptability.

Figure 5

Reduction of data protection costs. N = 54



Source: compiled by the author

Following this question, if respondents answered “yes”, they were invited to elaborate on what kind of tools their company is using to minimize costs while remaining compliant. The responses revealed a diverse set of strategies and initiatives that were being explored by or already implemented in the companies. To start, strategies such as data minimization, encryption, and developing clear retention policies were seen in several entries, which demonstrate a focus on efficient data management to reduce unnecessary storage and processing costs. Furthermore, a couple of answers mentioned embracing automation, artificial intelligence, and implementing automated filters for screening transaction data and sanctions screening systems, which reflects the commitment to leveraging technology for efficiency gains and cost savings. In addition, the reoccurring answer was employee training and awareness, which would prevent security incidents and minimize the need for costly incident response. Companies are also responding to exploring cloud migration as a cost-effective solution and optimizing cloud storage practices. This aligns with a broader trend in leveraging cloud technologies for scalability and cost efficiency. Thakkalapelli (2023) outlines the benefits of cloud migration for small businesses. These advantages include cost efficiency through the elimination of on-premises infrastructure, scalability to adjust resources based on demand, flexibility to adapt to market changes, and accessibility allowing for remote work and collaboration. However, the author also highlights challenges related to cloud migration, which

include concerns about data security, the complexity of integrating existing systems with cloud solutions, and the need for careful cost control to avoid overspending (Thakkalapelli, 2023).

Overall, the responses to the questionnaire indicate a diverse range of strategies and initiatives employed by the companies to minimize costs while ensuring compliance. Companies are adopting a multifaceted approach, which combines technological innovation, employee empowerment, and strategic decisions to strike a balance between cost reduction and compliance.

4. CONCLUSIONS AND RECOMMENDATIONS

1. After conducting a thorough analysis of the scientific literature on the topic of anti-money laundering and data protection for companies and the opportunities for reduction it can be concluded that companies face various financial burdens to comply with ever-changing anti-money laundering regulations as well as protecting data of the customers. Literature highlights that compliance costs are on the rise due to the constantly changing regulatory landscape, geopolitical uncertainties, and the dynamic nature of evolving financial crimes. The global impact of AML regulations is evident in variations across regions, such as Europe and Asia. The challenges were further intensified by the COVID-19 pandemic, affecting sanction screening, and labor expenses, and necessitating adaptations to cope with the increased instances of financial crime.
2. The GDPR implementation in 2018 caused a significant increase in staff costs for European Union companies, which contrasted with a smaller increase detected in the United States. Furthermore, an in-depth examination was examined regarding the repercussions of non-compliance, implying the significant average costs associated with data breaches in the year 2022. This underscores the considerable financial strain on entities and the ensuing ripple effect affecting consumers.
3. The examination of existing literature brings attention to diverse approaches aimed at diminishing compliance expenditures in both anti-money laundering and data protection protocols. Notably, the utilization of artificial intelligence, robotic process automation, and natural language processing emerge as a promising strategy to augment operational efficiencies and alleviate costs linked to regulatory adherence. Additionally, the literature emphasizes the hurdles confronted by financial institutions in the realm of AML, including outdated controls, inadequate regulatory backing for innovation, and inefficiencies in reporting mechanisms.
4. The quantitative approach used in the thesis estimated two main models to test the relationship between two dependent variables – anti-money laundering costs and data protection costs and other independent variables such as asset size, anti-money laundering awareness and efforts, and region and industry dummy variables. The findings indicated that there is a significant linear relationship between the size of the company and the company's portion of costs allocated to anti-money laundering compliance and data protection. Furthermore, companies with higher awareness levels experience higher costs related to anti-money laundering and data protection measures,

while companies investing in data protection measures experience lower costs with AML and data protection compliance. Finally, data protection costs are positively correlated with anti-money laundering costs, which shows synergy and interdependence between strategic investments and initiatives of data protection and efforts to combat financial crime and comply with anti-money laundering regulations.

5. The qualitative approach used in the thesis aimed to investigate the answers of surveyed companies that were not included in the models in the quantitative approach phase of the thesis. regulations are the most challenging part when dealing with anti-money laundering compliance, followed by costs. In addition, data protection measures used by the surveyed companies were analyzed. The findings show that companies are most likely to use encryption and employee training as their data protection tools. This stage also analyzed data breaches and security incidents the companies elaborated on in the survey. Findings showed that only a minority of the respondents experienced such incidents from which phishing incidents were the most common ones. Finally, the reduction of costs part was analyzed. Findings portrayed that a variety of strategies is being explored by the surveyed companies, such as technological advancements, employee empowerment, and strategic decision-making to achieve an equilibrium between cost reduction and adherence to the regulations.

For further analysis, it would be beneficial to collect more respondents account for a small response rate, and expand the sample size. A larger and more diverse sample size would enhance the generalizability of the findings. Including a broader range of companies from various industries, sizes, and countries would provide a more comprehensive understanding of the complexities surrounding anti-money laundering and data protection costs. Furthermore, it would be beneficial to consider investigating trends over time. It would allow further research to observe changes, adaptations, and emerging patterns in how companies address anti-money laundering and data protection costs over different periods. In addition, integrating more qualitative research methods such as interviews and case studies would provide a deeper understanding of companies' experiences, which would enhance quantitative findings as well.

REFERENCES

1. A. Frazzetto. (2022). *5 ways to reduce compliance costs with AI and automation*. https://www.cio.com/article/350250/5-ways-to-reduce-compliance-costs-with-ai-and-automation.html
2. Al Habsyi, S., Suharman, H., & Handoyo, S. (2021). Effect Of GRC and Intellectual Capital on Company Performance. *Jurnal Riset Akuntansi Kontemporer, 13(2)*, 106–112.
3. AML RightSource. (2020). *Why five Dutch banks are teaming up to counter money laundering*. https://www.amlrightsource.com/news/why-five-dutch-banks-are-teaming-up-to-counter-money-laundering/
4. Anant, V., Donchak, L., Kaplan, J., & Soller, H. (2020). The consumer-data opportunity and the privacy imperative. In *McKinsey & Company.* . https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative
5. Baig, A. (2022). Top 4 Benefits of Using Data Encryption for Businesses. . *Digital Marketing News*. https://www.dmnews.com/benefits-of-data-encryption/
6. Bortolotti, R. (2018). Data Prep 2-2: Dummy Coding Category Variables. In *Handbook of Statistical Analysis and Data Mining Applications (Second Edition)*. https://www.sciencedirect.com/topics/computer-science/categorical-variable
7. Centre for Information Policy Leadership. (2023). *Business Benefits of Investing in Data Privacy Management Programs.* https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cisco-cipl_report_on_business_benefits_of_investing_in_data_privacy_management_programs__10_jan_2023_.pdf
8. Chen, C., Frey, C. B., & Presidente, G. (2022). *Privacy regulation and firm performance: Estimating the GDPR effect globally* (The Oxford Martin Working Paper Series on Technological and Economic Change).
9. Ciancimino, J. (2023). *Regulatory Compliance Costs & How It Helps Your Bottom Line* . I.S. Partners SOC . https://www.ispartnersllc.com/blog/rising-compliance-costs/
10. Clyde Wayne Crews, Jr. (2018). *Ten Thousand Commandments. An annual Snapshot of the Federal Regulatory State*. https://cei.org/sites/default/files/Ten_Thousand_Commandments_2018.pdf#page=18

11. ComplyAdvantage. (2019). *Layering in AML - What Is Layering In Money Laundering?* . https://complyadvantage.com/insights/money-laundering-layering/
12. ComplyAdvantage. (2021). *Anti Money Laundering History: 1970 to 2022.* .
13. DesJardins, J. (2013). *An Introduction to Business Ethics*.
14. Dzhaparov, P. (2022). Artificial Intelligence-a Key Success Factor for Wealth Management Industry. In *Известия на Съюза на учените-Варна. Серия Икономически науки, 11(2)* (pp. 97–104).
15. European Anti-Fraud Office. (2023). *BELENOS: €18 million of illicit cash flows uncovered across Europe in two weeks.* https://anti-fraud.ec.europa.eu/media-corner/news/belenos-eu18-million-illicit-cash-flows-uncovered-across-europe-two-weeks-2023-11-16_en
16. European Data Protection Supervisor. (n.d.). *The History of the General Data Protection Regulation.* Retrieved December 14, 2023, from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en#:~:text=In%202016%2C%20the%20EU%20adopted,as%20law%20across%20the%20EU.
17. European Parliament. (2023). *New EU measures against money laundering and terrorist financing.* Press Releases ECON. https://www.europarl.europa.eu/news/en/press-room/20230327IPR78511/new-eu-measures-against-money-laundering-and-terrorist-financing
18. European Union. European Data Protection Supervisor. (2012). *Opinion of the European Data Protection Supervisor*. https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf
19. Eurostat. (2023). NACE Background. In *Statistics Explained* . https://ec.europa.eu/eurostat/statistics-explained/index.php?title=NACE_background#Structure_and_coding_of_NACE
20. Fairburn, L. (n.d.). *The Importance and Benefits of Incident Response.* . Pentest People Ltd. Retrieved December 14, 2023, from https://www.pentestpeople.com/blog-posts/the-importance-and-benefits-of-incident-response#:~:text=Benefits%20of%20an%20Incident%20Response%20Plan&text=Quickly%20assess%20the%20impact%20of%20cyber%20threats%20%26%20take%20corrective%20measures.&text=Identify%20the%20root%20cause%20of,prevent%20similar%20incidents%20in%20future.&text=Restore%20normal%20operations%20%26%20prot

ect%20data%20from%20further%20loss%20or%20misuse.&text=Improve%20cyber%20security%20posture%20and%20compliance.

21. Ferwerda, J. (2018). The effectiveness of anti-money laundering policy: a cost-benefit perspective. In *The Palgrave Handbook of Criminal and Terrorism Financing Law* (pp. 317–344).
22. Financial Action Task Force. (n.d.-a). *FATF Recommendations* . Retrieved December 13, 2023, from https://www.fatf-gafi.org/en/topics/fatf-recommendations.html
23. Financial Action Task Force. (n.d.-b). *History of Anti-Money Laundering Laws.* . Retrieved December 13, 2023, from https://www.fincen.gov/history-anti-money-laundering-laws
24. Financial Crimes Enforcement Network. (2023). *Bank Secrecy Act Advisory Group; Solicitation of Application for Membership.* . https://www.federalregister.gov/documents/2023/02/13/2023-02977/bank-secrecy-act-advisory-group-solicitation-of-application-for-membership
25. FinTech Global. (2023). *Rising AML compliance costs to impact financial institutions significantly.* https://fintech.global/2023/10/03/rising-aml-compliance-costs-to-impact-financial-institutions-significantly/
26. Forrester Consulting. (2023). True Cost Of Financial Crime Compliance Study, 2023. In *A Forrester Consulting Thought Leadership Paper commissioned by LexisNexis® Risk Solutions.* https://risk.lexisnexis.com/global/en/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report
27. Friedrich, C., & Quick, R. (2019). An analysis of anti-money laundering in the German non-financial sector. *Journal of Management and Governance, 23(4)*, 1099–1137.
28. Frost, J. (n.d.-a). *Overfitting Regression Models: Problems, Detection, and Avoidance.* . Statistics By Jim. . Retrieved December 14, 2023, from https://statisticsbyjim.com/regression/overfitting-regression-models/
29. Frost, J. (n.d.-b). *Root Mean Square Error (RMSE).* Statistics By Jim. . Retrieved December 14, 2023, from https://statisticsbyjim.com/regression/root-mean-square-error-rmse/
30. Gryszczyńska, A. (2021). The impact of the COVID-19 pandemic on cybercrime. In *Bulletin of the Polish Academy of Sciences: Technical Sciences.*
31. Gurule, J. (1995). The Money Laundering Control Act of 1986: Creating a New Federal Offense or Merely Affording Federal Prosecutors an Alternative Means of Punishing

Specified Unlawful Activity? *List American Criminal Law Review*. https://scholarship.law.nd.edu/law_faculty_scholarship/21

32. Han, J., Huang, Y., Liu, S., & Towey, K. (2020). Artificial intelligence for anti-money laundering: a review and extension. In *Digital Finance, 2(3-4)* (pp. 211–239).
33. Handoko, B. L., Riantono, I. E., & Gani, E. (2020). Importance and benefit of application of governance risk and compliance principle. In *Systematic Reviews in Pharmacy, 11(9)* (pp. 510–513).
34. Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law 28 (1)*, 65–98.
35. Huddleston, J. (2021). The Price of Privacy: The Impact of Strict Data Regulations on Innovation and More. In *American Action Forum* . https://www.americanactionforum.org/insight/the-price-of-privacy-the-impact-of-strict-data-regulations-on-innovation-and-more/
36. IBM. (n.d.). *What is GRC?* . Retrieved December 14, 2023, from https://www.ibm.com/topics/grc
37. IBM Security. (2021). *Cost of a Data Breach Report 2021*. https://www.dataendure.com/wp-content/uploads/2021_Cost_of_a_Data_Breach_-2.pdf
38. IBM Security. (2023). *Cost of a Data Breach Report 2023*. https://www.ibm.com/downloads/cas/E3G5JMBP
39. Ilahi, A. H. A., & Widowaty, Y. (2021). The optimization of corruption deterrence during the Covid-19 Pandemic. *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law), 8(1)*, 71–91.
40. Jackie Wheeler. (2023). *Guidance on Anti-Money Laundering (AML) in Banking and Finance for 2023*. https://www.jumio.com/aml-guidance-banking-finance/
41. Jendruszak, B. (2023). *What Is Layering In Money Laundering & How Does It Work?* . https://seon.io/resources/layering-money-laundering/
42. Jia, J., Jin, G. Z., & Wagman, L. (2021). The short-run effects of the general data protection regulation on technology venture investment. In *Marketing Science, 40(4)* (pp. 661–684).
43. Johari, R. J., Zul, N. B., Talib, N., & Hussin, S. A. H. S. (2020). *Money laundering: Customer due diligence in the era of cryptocurrencies. 1st International Conference on Accounting, Management and Entrepreneurship (ICAMER 2019) (pp. 130-135). Atlantis Press.*

44. Kaya, C. T., Türkyılmaz, M., & Birol, B. (2019). Impact of RPA technologies on accounting systems. In *Muhasebe ve Finansman Dergisi*.

45. Koski, H., & Valmari, N. (2020). *Short-term Impacts of the GDPR on Firm Performance (No. 77)*.

46. Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons, 64(5)* , 659–671.

47. Levi, M., & Reuter, P. (2006). *Money Laundering*. http://www.jstor.org/stable/10.1086/501508

48. LexisNexis Risk Solutions. (2016). *Financial Transparency and Inclusion Survey*. https://risk.lexisnexis.com/global/en/insights-resources/research/financial-transparency-and-inclusion-survey

49. LexisNexis Risk Solutions. (2021). *True Cost Of Financial Crime Compliance Study. Global Report.* https://risk.lexisnexis.com/global/en/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report

50. LexisNexis Risk Solutions. (2022). *2022 APAC True Cost of Financial Crime Compliance Study*. https://risk.lexisnexis.com/global/en/insights-resources/research/true-cost-of-financial-crime-compliance-study-apac

51. Lisanawati, G., & Sadeghi, M. (2019). Disclosure Of Data Related To Money Laundering Investigation From Data Protection Perspective. . In *NFCT Nilai Field Consultancy and Training: Qualitative and Quantitative Research Review, 4(1)* (pp. 179–191).

52. Lord, N. (2022). *What is the Data Protection Directive? The Predecessor to the GDPR*. Data Insider. Digital Guardian's Blog. https://www.digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr#:~:text=Definition%20of%20the%20Data%20Protection,free%20movement%20of%20such%20data.

53. McCombes, S. (2023). Sampling Methods | Types, Techniques & Examples. . In *Scribbr.* . https://www.scribbr.com/methodology/sampling-methods/

54. McQuinn, A., & Castro, D. (2019). The Costs of an Unnecessarily Stringent Federal Data Privacy Law. Information Technology & Innovation Foundation. In *Information Technology & Innovation Foundation.* . https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law/

55. Mohammad, S. J., Tahtamouni, A., Aldaas, A. A., & Sumadi, M. A. (2022). *Preventing money laundering during the placement stage: the Jordanian commercial banks case.International Journal of Public Law and Policy* (8(1)).

56. Nance, M. T. (2018). *The regime that FATF built: an introduction to the Financial Action Task Force. Crime, Law and Social Change*.

57. Onfido. (2023). *Importance of Anti-Money Laundering.* . https://onfido.com/blog/importance-of-anti-money-laundering/

58. Ponemon Institute. (2022). *2022 Cost of a Data Breach Report*. https://securityintelligence.com/series/2022-cost-of-a-data-breach-report/#articles

59. Ponemon Institute LLC. (2017). *The True Cost of Compliance with Data Protection Regulations: Benchmark Study of Multinational Organizations.* https://static.fortra.com/globalscape/pdfs/guides/gs-true-cost-of-compliance-data-protection-regulations-gd.pdf

60. Pontes, R., Lewis, N., McFarlane, P., & Craig, P. (2022). Anti-money laundering in the United Kingdom: new directions for a more effective regime. *Journal of Money Laundering Control, 25(2)*, 401–413.

61. Privacy Engine. (2023). *Data Protection Training with IAPP – Everything You Need To Know.* https://www.privacyengine.io/blog/data-protection-training/#:~:text=Enhanced%20compliance%3A%20Data%20protection%20training,data%20breaches%20and%20associated%20costs

62. Qi, C. C. (2020). Big data management in the mining industry. *International Journal of Minerals, Metallurgy and Materials, 27*, 131–139.

63. Radosavljevic, L. (2021). Security and Privacy Requirements in the Public Utility Space. In *Helpy.io, Inc.* . https://helpy.io/blog/security-and-privacy-requirements-in-the-public-utility-space/

64. Randhawa, A., Rogers, L., & Davies, M. (2022). How to navigate the increase in financial crime risks during a downturn. In *White & Case LLP.* . https://www.whitecase.com/insight-our-thinking/mining-metals-2022-how-navigate-increase-financial-crime-risks-during-downturn

65. Smith, A., & Boddy, M. (2020). Economic Crime in the Manufacturing Sector. In *Deloitte LLP.* https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/corporate-finance/deloitte-uk-economic-crime-manufacturing.pdf

66. Soetewey, A. (2021). *Multiple linear regression made simple*. Stats and R. . https://statsandr.com/blog/multiple-linear-regression-made-simple/#multiple-linear-regression

67. Telecom Review. (2021). *Data in telecom: key asset and key risk.* . The Telecoms Industry Media Platform. . https://www.telecomreview.com/articles/reports-and-coverage/5263-data-in-telecom-key-asset-and-key-risk

68. Thakkalapelli, D. (2023). Cost Analysis of Cloud Migration for Small Businesses. *Tuijin Jishu/Journal of Propulsion Technology, 44(4)*, 4778–4784.

69. Truskauskas, G., & Taujanskaitė, K. (2022). Efficiency of anti-money laundering: the case of Northern European Countries. In *Business and management* (pp. 430–440).

70. van Egmond, M. B., Rooijakkers, T., & Sangers, A. (2021). Privacy-Preserving Collaborative Money Laundering detection. In *ERCIM NEWS, 27.*

71. White, K. R. (2020). *The Cost of Big Data: Evaluating the Effects of the European Union's General Data Protection Regulation*.

72. Wolford, B. (n.d.). *What is GDPR, the EU's new data protection law?* GDPR.EU. Retrieved December 13, 2023, from https://gdpr.eu/what-is-gdpr/?cn-reloaded=1

73. Zaeem, R. N., & Barber, K. S. (2020). *The effect of the GDPR on privacy policies: Recent progress and future promise* .

ANNEXES

Annex 1

Questionnaire

AML (Anti-Money Laundering) and Data Protection Costs
All information provided will be kept strictly confidential and will only be used for academic purposes. Thank you for the contribution!

* Indicates a required question

1.

Primary Location of the Company (Country)

*

Industry Sector (based on NACE codes)

*

Mark only one oval.

A - Agriculture, forestry and fishing
B - Mining and quarrying
C - Manufacturing
D - Electricity, gas, steam and air conditioning supply
E - Water supply; sewerage; waste managment and remediation activities
F - Construction
G - Wholesale and retail trade; repair of motor vehicles and motorcycles
H - Transporting and storage
I - Accommodation and food service activities
J - Information and communication
K - Financial and insurance activities
L - Real estate activities
M - Professional, scientific and technical activities
N - Administrative and support service activities
O - Public administration and defence; compulsory social security
P - Education
Q - Human health and social work activities
R - Arts, entertainment and recreation
S - Other services activities
T - Activities of households as employers; undifferentiated goods - and services - producing activities of households for own use
U - Activities of extraterritorial organisations and bodies
Other (please specify in the next question)

3.

Required If Selected Other: specify industry

4.

Asset Size (Select the approximate range)*

Mark only one oval.

Less than €2 million
€2 million - €10 million
€10 million - €50 million
€50 million - €100 million
€100 million - €250 million
More than €250 million

5.

Does your company have a dedicated AML compliance department or officer?

*

Check all that apply.

Yes

No

Other:

6.

If you answered **Yes** in the last question: How many employees dedicated to the AML compliance does your company have?*

7.

What is the approximate annual cost of implementing and maintaining your AML compliance measures?

*

Mark only one oval.

Less than €10,000

€10,000 - €25,000

€25,000 - €50,000

€50,000 - €100,000

Over €100,000

8.

How would you rate your company's current AML compliance efforts?

*

Mark only one oval.

Very Poor

1

2

3

4

5

Excellent

9.

Are you aware of the regulatory requirements related to AML in your industry?

*

Mark only one oval.

Yes

No

10.

What challenges or obstacles does your company face when it comes to AML compliance? (Open-ended)

*

11.

Does your company invest in data protection and cybersecurity measures?

*

Mark only one oval.

Yes

No

12.

On a scale of 1 to 5, how concerned is your company about data breaches and data protection costs, with 1 being not concerned and 5 being extremely concerned?

*

Mark only one oval.

not concerned

1

2

3

4

5

extremely concerned

13.

What types of data protection measures does your company currently employ? (Select all that apply)

*

Check all that apply.

Encryption
Employee Training
Regular Audits
Access Controls
Data Backup
Incident Response Plan
Other:

14.

What is the approximate annual cost of implementing and maintaining your data protection and cybersecurity compliance measures?

*

Mark only one oval.

Less than €10,000
€10,000 - €25,000
€25,000 - €50,000
€50,000 - €100,000
Over €100,000

15.

Have you experienced any **data breaches** in the past two years? If yes, please briefly describe the incident. (Open-ended)

*

16.

Have you experienced any **security incidents** in the past two years? If yes, please briefly describe the incident. (Open-ended)

*

17.

Is your company actively exploring opportunities to reduce data protection costs while maintaining security?

*

Mark only one oval.

Yes

No

Other:

18.

What strategies or initiatives has your company considered or implemented to reduce data protection costs? (Open-ended)

*

19.

Is there any additional information or comments you would like to provide related to AML compliance, data protection costs, or your company's approach to these issues? (Open-ended)

Confirmation message

Thank you for participating in this survey. Your responses will remain completely anonymous, and your input is highly valuable to my research.