National College of Ireland

Project Submission Sheet

Student Name:	Erica Castillo Gonzalez
Student ID:	24155233
Programme:	MSc in Entrepreneurship **Year:** 2025
Module:	Dissertation
Lecturer:	Jeffrey Walsh
Submission Due Date:	15th August 2025
Project Title:	Artificial Intelligence in Anti-Money Laundering: Opportunities, Threats, and the Operational Challenges Facing Financial Institutions
Word Count:	18132

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
<u>ALL</u> internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature:

Date: 15th august 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

Office Use Only	
Signature:	
Date:	

Penalty Applied (if applicable):	

AI Acknowledgement Supplement

Dissertation

Artificial Intelligence in Anti-Money Laundering: Opportunities, Threats, and the Operational Challenges Facing Financial Institutions

Your Name/Student Number	Course	Date
24155233	MSc in Entrepreneurship	15th august 2025

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool
NotebookkLM	AI tool used for organizing research notes and generating summaries	https://notebooklm.google.com/
Deepl	AI-powered translation tool used for translating and refining text between Spanish and English	https://www.deepl.com/es/translator
ChatGPT	Used for language refinement and clarity checks	https://chat.openai.com/

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

[Insert Tool Name] NotebookkLM	
[Insert Description of use] AI tool used for organizing research notes and generating summaries	
[Insert Sample prompt]	[Insert Sample response]

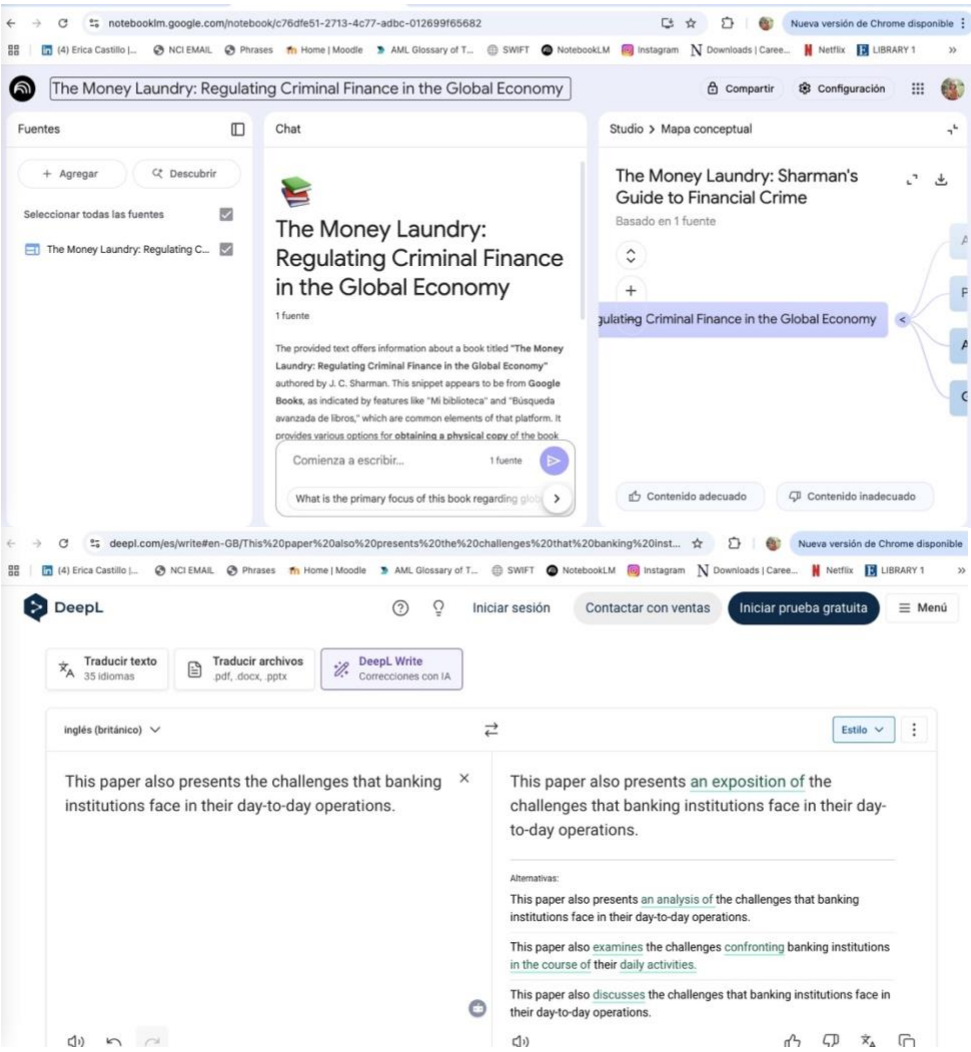
[Insert Tool Name] Deepl	
[Insert Description of use] AI-powered translation tool used for translating and refining text between Spanish and English	
[Insert Sample prompt]	[Insert Sample response]

[Insert Tool Name] ChatGPT	
[Insert Description of use] Used for language refinement and clarity checks	
[Insert Sample prompt]	[Insert Sample response]

Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

Additional Evidence:



chatgpt.com/g/g-p-683f22f518a48191b9283e25db3b43b3-tesis/c/689f1860-ca88-8327-b8dc-c060605beb8e

Nueva versión de Chrome disponible

(4) Erica Castillo |... NCI EMAIL Phrases Home | Moodle AML Glossary of T... SWIFT NotebookLM Instagram Downloads | Caree... Netflix LIBRARY 1

ChatGPT 5

Compartir

explain me, in very simple terms what is a black box in AML terms?

Sure — in very simple terms:

In AML, a **black box** is like a machine that tells you *"This transaction looks suspicious"* but **doesn't tell you why**.

You see the answer, but you can't see what's going on inside or how it decided that. That makes it hard for banks to explain the decision to regulators or check if the machine is right.

ABSTRACT

This study explores how financial institutions are currently leveraging artificial intelligence (AI) in the fight against money laundering criminal organisations. It examines the extent to which AI serves as a powerful tool for identifying patterns, behaviors, and warning signals indicative or illicit activities within an increasingly interconnected global banking system.

The research outlines the three stages of money laundering, highlights activities identified as illicit by international organisations and discusses the consequences of criminal groups continuing to bypass regulatory filters and infiltrate the global financial market. It also explores the day-to-day challenges faced by banking institutions in managing such threats.

Furthermore, this study seeks to provide evidence supporting the argument that AI can be a valuable tool in accelerating the detection of suspicious transactions, reinforcing the security filters of the global financial system, and reducing the proportion of criminal funds circulating within it. Most importantly, it explores how improving the fight against money laundering can lead to a significant reduction in the financial resources available to criminal organisations engaged in activities such as human trafficking, illegal drug trade, terrorism, and other serious offences.

This research provides a relevant contribution by examining practical insights from industry professionals in the context of global regulatory frameworks and technological advancements in AML. By aligning first-hand perspectives with existing international developments, the study aims to highlight connections between operational realities and broader policy and innovation trends, offering a grounded understanding of how artificial intelligence can enhance and potentially challenge AML frameworks.

Submission of Thesis and Dissertation

National College of Ireland
Research Students Declaration Form
(Thesis/Author Declaration Form)

Name: Erica Castillo González

Student Number: 24155233

Degree for which thesis is submitted: MSc in Entrepreneurship

Title of Thesis: Artificial Intelligence in Anti-Money Laundering: Opportunities, Threats, and the Operational Challenges Facing Financial Institutions

Date: 15/08/2025

Material submitted for award

A. I declare that this work submitted has been composed by myself. X

B. I declare that all verbatim extracts contained in the thesis have been distinguished by quotation marks and the sources of information specifically acknowledged. X

C. I agree to my thesis being deposited in the NCI Library online open access repository NORMA. X

D. ***Either*** *I declare that no material contained in the thesis has been used in any other submission for an academic award.
Or *I declare that the following material contained in the thesis formed part of a submission for the award of

Master of Science in Entrepreneurship

(State the award and the awarding body and list the material below)

ACKNOWLEDGEMENT

To Ireland, for embracing me and giving me the space to grow, to dream, and to challenge myself in ways I never imagined.

To my brother and my mum, for their unwavering faith in me, even in moments when I doubted myself. Your belief has been the steady strength behind every chapter of this journey.

And above all, to my Dad – for teaching me inner strength, for all the love and wisdom that still light my path. You are in every sunrise, in every flower, and in me – always and forever.

TABLE OF CONTENTS

CHAPTER 1 – INTRODUCTION

Statement of the Problem

In 2024, the organisation Nasdaq Verafin (2024), reported that, in 2023, more than 3 trillion dollars derived from illicit activities were successfully integrated and circulated within the global financial system. According to the United Nations Office on Drugs and Crime (UNODC), it is estimated that between 2% and 5% of the global gross domestic product (GDP) is associated with money laundering activities.

These figures reveal the magnitude of the threat posed by financial crime to global economic stability, and the reason why institutions around the world, along with private organisations, have joined forces to design strategies that help detect and disrupt the criminal networks behind illicit financial flows. These funds, generated through activities such as drug trafficking, corruption, fraud, or terrorism, area processed and disguised to appear legitimate within the financial system. According to the Financia Action Task Force (FATF, 2023), this process is defined as money laundering, which involves "*processing criminal proceeds to disguise their illegal origin*" and thereby allowing their use in the legitimate economy.

Although various international organisations and governmental bodies have developed regulatory frameworks and adopted technological advancements to combat this issue, the infiltration of criminal proceeds into legitimate financial systems remains a persistent challenge. The continuous evasion of financial security controls by organised criminal networks reduces the integrity of the global financial infrastructure. This ongoing circumvention enables a sustained flow of illicit funds, which not only support but also expand criminal operations across borders.

As a result, a self-reinforcing cycle emerges one in which illicit activities are perpetuated and expanded through continued access to legal financial channels. According to Nasdaq (2024), it is estimated that 782.90 billion USD originate from drug trafficking, 346.70 billion USD from human trafficking, 11.50 billion USD from terrorism related activities, and 485.60 billion USD from fraud. These alarming statistics highlight the urgent need for more advanced and adaptive mechanisms to detect and prevent money laundering at scale.

Research Question

What are the key challenges financial institutions encounter in the global landscape of anti-money laundering (AML), and to what extent can artificial intelligence (AI) function as both an enabler and a potential threat in enhancing AML frameworks?

Aim

To analyze the main challenges faced by financial institutions in the global fight against money laundering and to critically assess the dual role of artificial intelligence as both a facilitator and a potential risk in strengthening AML frameworks, linking practical findings with global regulatory and technological developments.

Objectives

- To identify the most significant operational, regulatory, and technological challenges hindering the effective implementation of AML measures in financial institutions.
- To examine current applications of artificial intelligence in AML processes.
- To evaluate the benefits, limitations, and potential risk associated with AI adoption in AML frameworks.
- To analyze the influence of global regulatory and compliance requirements on the integration of AI into AML efforts.
- To propose strategic recommendations for optimizing AI adoption, addressing the identified challenges, and mitigating associated risk.

Research Justification

Money laundering is a global threat that affects all industries and sectors of society. However, its consequences disproportionately impact the most vulnerable population. Beyond the financial dimension, money laundering presents a serious obstacle from multiple perspectives, including social harm, institutional weakening, international relations, and both micro and macroeconomics stability.

According to the International Labour Organization (ILO, 2005), it is estimated that 2.45 million people worldwide are exploited through human trafficking, many of whom are subjected to forced labour or commercial sexual exploitation. Significantly 43% of these victims are forced into the sex industry, while an estimated 40% to 50% are believed to be under 18. However, this figure is likely underestimated due to inconsistent age documentation. Human trafficking is also closely linked to legal economics sector, with approximately 32% of victims exploited in commercial activities such as agriculture, manufacturing, and domestic work. These realities underline the urgent need for more innovative approaches that go beyond traditional compliance measures. By integrating real-world perspectives from financial sector professionals with an analysis of the global regulatory and technological trends, this study seeks to generate insights that can inform more adoptive and effective AML strategies. The following chapters present the literature review, methodology, findings, discussion, and conclusion

CHAPTER 2 – LITERATURE REVIEW

Introduction to the Literature Review

This research begins by looking at the concept of money laundering and the three key stages commonly used to describe the process: placement, layering, and integration (FATF). Although often framed in strictly financial or legal terms, it is also a process though which criminal groups camouflage the illegal origin of their profits, enabling them to gain power, expand their networks, and penetrate legitimate sectors of the economy.

The impact of money laundering on the global financial system is both profound. When illicit founds are injected into formal economies, markets across various industries become distorted, and financial institutions are exposed to high reputational and operational risk. These dynamics weaken public trust in regulatory system and democratic institution, particularly in countries where oversight mechanism is fragile or politicised (World Bank 2022).

Beyond its financial and institutional consequences, money laundering has a devastating human cost. The funds being laundered often originate from crimes such as human trafficking, drug smuggling, corruption, or arms trading (UNODC 2021). These illicit flows directly impact vulnerable groups, especially children, women, and communities in developing countries who are exploited or displaced in the process. Addressing money laundering is therefore also a matter of protecting human rights.

Although various frameworks have been developed to address this global issue, most notably by the FATF, which includes over 200 jurisdictions (FATF 2024), significant gaps remain in the global anti-money laundering (AML) system. Multilateral organisations such as the World Bank, which aids developing countries in strengthening financial integrity (World Bank) and the International Monetary Fund (IMF), which support member states in enhancing AML frameworks have long supported countries in strengthening their regulatory capacity, yet criminal networks continue to exploit fragmentation and technological lag across borders.

In recent years, however, new tools have emerged. The rise of AI in financial services is reshaping the way AML processes are designed and implemented. From transaction monitoring to suspicious activity reporting, AI offers the potential to improve the speed, accuracy, and adaptability of compliance system, closing long-standing gaps exploited by criminals.

Definition and Scope of Money Laundering

The United Nations Office on Drugs and Crime (UNODC) defines money laundering as *"the processing of criminal proceeds to disguise their illegal origin"*. This definition highlights the importance of the process, as it allows criminal organisations to safeguard their financial gains and benefit from the profit of their illicit activities without exposing themselves to legal consequences.

In contrast, The International Organisation Bank for International Settlements (BIS), through the Basel Committee on Banking Supervision (2017), describes money laundering as the abuse of the financial system by criminal organisations, who use financial institutions either intentionally or not to introduce in the system illegal funds. This view, highlights not only on concealing the origin of the money, but also on the responsibility of the banking sector to implement strong internal controls, risk-based assessments, and due rigorous processes to prevent being used as vehicles for organised crime.

Finally, from an operational and systemic risk perspective, the U.S. Department of the Treasury (FinCEN) defines money laundering as financial transactions in which criminals attempt to disguise the origin, nature or source of illicitly funds. This definition underscores that laundering not only facilitates a wide range of serious criminal offences, but also poses a direct threat to the integrity of the financial system (U.S. Department of the Treasury, n.d.).

Considering the definitions explored, the definition proposed by the BIS, through the Basel Committee on Banking Supervision, more accurately reflects the vulnerability of the financial sector in relation to money laundering. This interpretation not only highlights the responsibility of institutions to implement internal measures and controls, but also positions the sector as a key actor, almost functioning as a form of financial law enforcement tasked with detecting, preventing, and reporting illicit activity. This responsibility does not rest solely on the institution, but also extent to its employees, who must remain constantly vigilant in their day-to-day operations. Consequently, money laundering is not merely a threat to the economic system, but also to the social and political system, turning financial institutions into a central pillar in the broader fight against organised crime. This constant pressure requires financial entities not only to invest in technology and staff training, but also to reassess their compliance strategies and risk management frameworks (Lucinity, 2025).

After establishing the concept of money laundering from several leading institutional perspectives, it is essential to examine how this crime operates in practices. According to most jurisdiction and international bodies, the money laundering process typically consists of three main stages. This research, adopts the FATF framework, widely recognised by regulatory and financial institutions.

- Placement – the initial stage, refers to the act of inserting proceeds from illicit activities into the formal financial systems. Criminal organisations frequently break down large sums of cash into smaller amounts that can be deposited into bank accounts without attracting attention from authorities a practice better known as *smurfing* (Madinger, J. 2012). In addition, FATF highlights that these actors also use financial instruments such as cheques and money orders, which can similarly be deposited in small increments to avoid detection.
- Layering – the second stage, distances the funds from their illicit origin through a series of financial transactions. Launderers move money across accounts and jurisdiction, often using shell companies or fictitious transactions to obscure the audit trail. Weak regulations in certain countries make them attractive for hidings illicit gains (FATF, n.d.).
- Integration, the final stage reintroduced laundered founds into the economy as legitimate assets. At this point, the money has often crossed borders and passed through multiple institutions, complicating efforts to trace it. It is then invested in luxury goods, real estate, or legitimate business.

This three-stage model, illustrated by UNODC, shows how illicit funds are introduced, obscured, and legitimised through global financial systems.

Figure 1.

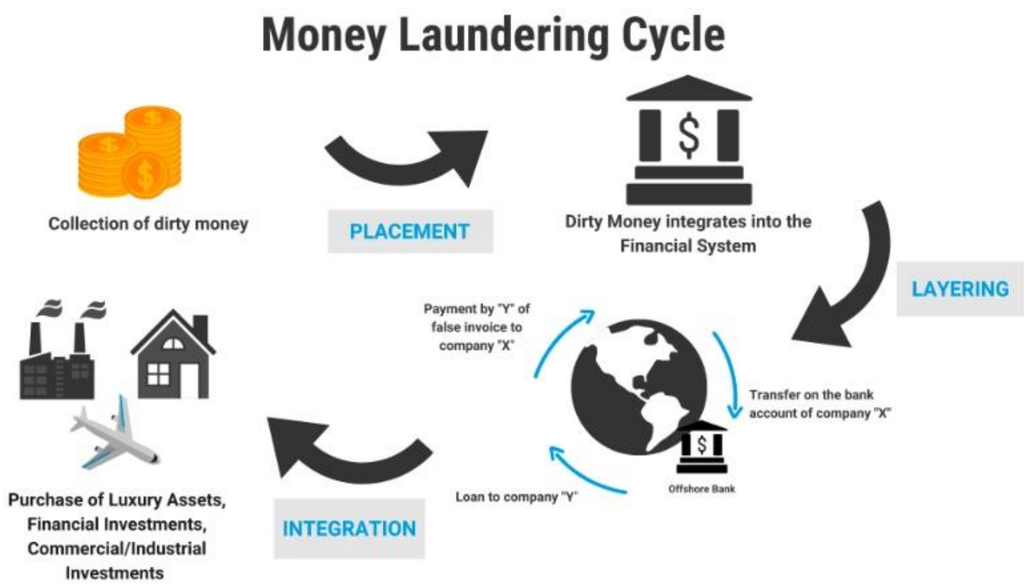


Figure 1. The Money Laundering Cycle. Source: United Nations Office on Drugs and Crime (UNODC).

Challenges in Detection and Prevention

An additional aspect that must be considered when analyzing money laundering is the wide range of challenges associated with its detection and prevention in a globalized financial environment. According to Levi, M. & Reuter, P. (2006), one of the most significant difficulties arises from the transnational nature of this offence, which enables criminal organisations to exploit discrepancies between legal systems and regulatory frameworks across jurisdictions.

Criminal organisations often hire legal and financial experts to navigate regulations across jurisdictions, giving them a significant advantage in avoiding detection. This expertise makes it harder for regulators and banks to trace to their source.

An equally relevant dimension in addressing money laundering in the imperative of effective international cooperation. Unger and Van Der Linde (2013) highlight that criminal networks systematically exploit differences between national legal frameworks, regulatory capacities, and enforcement priorities to transfer funds across borders with minimal risk. Political sensitivities, institutional differences, and poor information-sharing channels limit mutual legal assistance and cross-border investigations.

Fragmented regulations make it harder to track transactions through multiple jurisdictions, allowing criminals to design complex corporate structures in countries with low transparency requirements. Furthermore, differences in the thresholds for reporting suspicious activity and in the applications of due diligence obligations contribute to an environment where regulatory arbitrage becomes a viable strategy for money launderers.

Therefore, strengthening international cooperation is not merely a supplementary measure but rather a central component of any effective anti-money laundering strategy. Only through harmonised regulations, shared intelligence, and sustained joint enforcement efforts can close the gaps that have long allowed illicit funds to flow across borders.

Consequences of Money Laundering in the Financial System

Money laundering perpetuates global inequality by disproportionately impacting developing economies. These jurisdictions can face losses equivalent to a significant share of their GDP, undermining public investment in essential sectors such as health, education, and infrastructure.

The diversion of resources away from productive uses not only constrains economic growth but also reduce public trust in financial institutions and governance structures. affect vulnerable population, the most visible structural effects lie in the erosion of trust, stability, and integrity within the banking sector (FATF, 2013).
Furthermore, the ongoing globalisation of the economy, coupled with the rapid expansion of digital technologies, has significantly increased both the complexity and the speed of cross-border financial transactions. These developments have generated considerable benefits in terms of international trade and financial inclusion (Levi, M. & Reuter, P. 2006).

Within this context, the banking system occupies a central role, acting simultaneously as a victim and in some cases, as an unwitting conduit for illegal activities. Although financial institutions operate under increasingly stringent regulatory frameworks and have adopted enhanced due diligence procedures, they continue to be targeted by sophisticated criminal network. These groups usually employ complex corporate structures, nominee arrangements, and cross-border transfers designed to avoid existing controls and the scrutiny of supervisory authorities. Nevertheless, in practice, factors such as information asymmetries, technological limitations, perverse incentives, and instances of corruption contribute to the emergence of breaches that enable illicit capital to enter and circulate within the formal financial system (Unger and Van Der Linde, 2013).

The persistence of these operations within banking institutions even those regarded as among the most robust in terms of compliance demonstrates that, despite significant regulatory progress and substantial investment in monitoring and reporting systems, money laundering remains an established threat. This reality continues to undermine the credibility of financial markets and erode the confidence of economic stakeholders (Levi, M. & Reuter, P., 2006).

One of the principal challenges faced by financial institutions lies in consolidating their position in the eyes of the public, clients, investors and regulatory bodies as organisations with a solid and favourable reputation. This positioning is not limited only to the implementation of compliance procedures aimed at combating money laundering, rather, it also involves demonstrating that the institutions is secure, trustworthy and capable of safeguarding the interests of its depositors and counterparties.

When internal monitoring and prevention controls are evaded by criminal organisations, the resulting consequences extent far beyond direct financial losses. As noted by Unger and Van Der Linde (2013), the reputational damage caused by such incidents represents a cost that is considerably more difficult to repair and often endures for many years. Once public perception has been compromised, it becomes extremely challenging to restore the confidence of investors and the international community. This erosion of institutional credibility typically triggers a series of negative repercussions, which not only undermine the financial stability of the organisation but also diminish its ability to inspire trust among both internal and external stakeholders.

The 2012 HSBC case illustrates the severe regulatory and reputational consequences that can arise from weak AML controls. Record fines imposed that year, along with sustained public scrutiny, not only impaired the bank's standing but also underscored the substantial cost linked to compliance failures (U.S. Senate, 2012). Such high-profile breaches can also erode broader market confidence, creating a contagion effect across the financial sector Levi (2012).

Extending this discussion beyond the structural damage, it is essential to acknowledge the broader human consequences. While institutions are often at the centre of anti-money laundering discussions, the individuals behind especially employees working in compliance or audit roles also experience significant risk. These professionals are frequently exposed to intense pressure, ethical dilemmas, and even threats to their personal safety when they attempt to confront or report suspicious activities. According to a 2022 analysis, compliance departments are facing persistent staffing shortages, with some banks unable to recruit or retain qualified personnel despite increasing regulatory demands. This lack of resources not only leads to burnout and excessive workloads among existing teams but also increases the personal and professional risk burned by compliance officers and senior executives (Buchalter, 2022). In extreme cases, the failure to detect laundering operations can result in job losses, legal implications, or professional discredit for individuals who may acted in good faith within flawed or overwhelming systems.

Moreover, money laundering intensifies existing global inequalities. In many cases, the victims of the criminal networks financed through laundered money such as women and children involved in trafficking or forced labour. These indirect victims often come from underdeveloped or conflict-affected regions, where systemic poverty, limited access to education, and weak governance create an environment in which criminal organisations can thrive. According to The World Bank, unintended consequences of global de-risking practices have led many international banks to terminate relationships with financial institutions in developing countries, particularly in the Latin America, sub-Saharan Africa, East Asia and South Asia. This trend driven by concerns over money laundering and regulatory penalties has further marginalised vulnerable populations by limiting their access to basic financial services and cross-border transactions (World Bank, 2018). Consequently, the very existence of a person can be shaped, or even condemned, by the place and conditions into which they are born.

Although international bodies have promoted standardised frameworks to combat illicit financial flows, the implementation of these measures often places disproportionate burdens on developing countries. These jurisdictions may be labelled as *"hight-risk"* or *"non-cooperative"* without a full understanding of their socio-economic realities or institutional limitations. Such classifications can damage their reputations, restrict access to global financial markets, and increase compliance cost ironically exacerbating the very vulnerabilities these measures aim to address.

Furthermore, these is an inherent tension between the push for global alignment and the need to respect the sovereignty of national systems. In practice, this dynamic can reinforce a cycle of dependency, where under-resourced nations struggle o meet externally imposed standards while being scrutinised under frameworks primarily designed by and for developed economies.

In this sense, money laundering is not only a financial crime, but also a mechanism that perpetuates global injustice. It allows those with illicit power to remain shielded while those with fewer resources, whether as professionals, citizen, or entire nations face the consequences of a system designed to monitor them more closely than it protects them.

Another significant challenge that financial institutions must address, both at microeconomic and macroeconomic levels, is the profound impact of illicit activities on the stability of economic systems. According to the International Monetary Fund (2001), illicit flows derived from money laundering represent between 2% and 5% of global GDP, which corresponds to an estimated USD 1 to 1.5 trillion annually. This constitutes an exceptionally large volume of funds actively circulating within international financial systems. Such flows undermine and devalue the global economic framework by weakening regulatory effectiveness, distorting competition and obstructing the development of strategic sectors.

As noted by Levi, M. & Reuter, P. (2006), criminal organisations are often able to sustain artificially low prices and assume greater risk because they rely on undeclared resources, thereby distorting competitive dynamics and undermining overall economic productivity. Furthermore, Global Financial Integrity (2017) has estimated that developing countries collectively lose approximately USD 1 trillion every year because of illicit financial flows, which intensifies unequally and restricts the scope for genuine investment. Taken together, these phenomena illustrate that money laundering represents not only a criminal offence but also a systemic threat to the integrity and resilience of both local and global financial markets.

Traditional Methods Used to Combat Money Laundering

Regulatory and Legal Frameworks

International efforts to combat ML gained momentum in the late 1980's, when the rapid expansion of transnational drug trafficking exposed critical weaknesses in financial oversight. The Vienna Convention of 1988 marked the first international agreement to classify ML as a criminal offence, initially linked to narcotics-related crimes, and ser a precedent for broader regulation. This was reinforced by the Palermo Convention of 2000, which extended the scope to cover laundering linked to any serious offence and promoted enhanced cross-border cooperation. Together, these conventions established the foundation for the global anti-money laundering framework and encouraged states to align their legal systems to address this transnational threat more effectively (Sharman, 2011).

Following the adoption of the Vienna and Palermo Convention, jurisdictions began developing their own legislation and regulatory measures. The Unites States, through the Bank Secrecy Act (1970), required financial institutions to collaborate with the government in detecting and preventing money laundering. Its provisions included maintaining transaction records, reporting cash operations exceeding USD 10,000, and filing Suspicious Activity Reports (SARs) in cases on unusual activity. The Act also introduced early Know Your Customer (KYC) procedures (Unger and Van Der Linde, 2013).

In Europe, the EU progressively developed directives to strengthen AML measures, moving from a uniform approach to a risk-based model. Directive (EU) 2015/849 introduced key elements such as enhanced scrutiny for high-risk sectors, while Directive 2018/843 expanded transparency on beneficial ownership and extended supervision to emerging sectors, including virtual asset service providers. These legal instruments underscored the EU's commitment to adapting regulatory frameworks to evolving financial crime risk while promoting cooperation among member states (European Union, 2015; European Union, 2018).

Following the initial period, which undoubtedly involved a process of trial and error, the FATF emerged on the international stage in 1989. This body, which operates independently of any specific jurisdiction, does not possess formal coercive powers. Nevertheless, it has exerted considerable influence through international pressure and initiatives such as the publication of blacklist. The primary purpose of these backlist is to assess whether jurisdictions have implemented effective anti-money laundering measures and whether they comply with established international standards. Although being placed on an FATF blacklist does not entail direct legal sanctions, it can lead to significant economic consequences, including restrictions on access to banking services, heightened scrutiny from international financial institutions, and a certain degree of financial isolation. As a result, many countries have been compelled to strengthen their compliance frameworks (Sharman, 2011). In addition to the FATF, other influential organisations perform similar roles. For example, the Egmont Group facilitates cooperations and information exchange among national Financial Intelligence Units, while the Basel Committee on Banking Supervision issues guidelines on banking supervision and customer due diligence. Collectively, these entities have contributed to consolidating stricter international expectations regarding the prevention of money laundering.

Governments and financial institutions have recognized that criminal organisations, including terrorist groups and drug trafficking networks, inevitably need to circumvent legal framework to introduce illicit funds into the formal economic system. This reality places banking institutions in a particularly vulnerable positions, as they may inadvertently become conduits for money laundering activities. To address this, standardised client categorisation and risk assessment procedures emerged, with KYC and Customer Due Diligence (CDD) becoming universal AML measures.

Know Your Customer (KYC) and Customer Due Diligence (CDD) risk scoring.

In order for a financial institution to formally initiate a business relationship, financial institutions are required to undertake a comprehensive identification and verification process of the natural or legal person seeking access to their services. The Know Your Customer (KYC) procedure entails the collection and validation of documentation that substantiates the client's identity and legal status, including full name, date of birth or incorporation, residential or business address. This information must be cross-verified for consistency and authenticity and screened against applicable regulatory lists to identity potential involvement in illicit activity or reputational concerns. KYC constitutes a foundational element of institutional risk management, serving not merely to confirm identify but also to assess the legitimacy of financial activities and to safeguard the financial system from abuse (Society for Worldwide Interbank Financial Telecommunication (SWIFT), n.d.; World Bank Group, International Finance Corporation, 2018).

Customer Due Diligence (CDD) builds upon the KYC framework adopting a more dynamic and risk-sensitive approach to evaluating potential threats associated with a client relationship. While KYC establishes the identity of the client, CDD seeks to determine the nature of the client's activities, the rationale for the relationship, and the extent to which their financial behavior conforms to expected patterns. It encompasses the verification of beneficial ownership in the case of legal entities, the assessment of the origin and legitimacy of funds, and the ongoing monitoring of transactions to detect anomalies indicative of illicit conducts (SWIFT, n.d.). This risk-based methodology categorises clients onto low, medium, or high-risk profiles, with enhanced measures applied proportionately to the assessed risk level. Although essential in practice, this reflexive approach may give rise to inconsistencies or unintended exclusion if not implemented with due rigor (World Bank Group, 2018).

To address procedural inefficiencies, industry-led initiatives such as the SWIFT KYC Registry have emerged as collaborative solutions. This registry, developed by the Society for Worldwide Interbank financial Telecommunication, is a global utility that enables financial institutions to upload, maintain, and share standardised KYC information securely with counterparties. It aims to streamline the onboarding process, reduce duplication, and improve transparency across jurisdictions (SWIFT, n.d.). However, these shared platforms do not exempt institutions from tailoring their CDD according to each client risk profile. As the International Finance Corporation (IFC) of the World Bank Group points out, CDD procedures must still reflect contextual factors and preserve institutional responsibility, even in environments where KYC utilities are adopted (World Bank Group, 2018).

Risk scoring operates in conjunction with KYC and CDD, enabling institutions to assign a quantitative or qualitative risk rating to each client based on variables such as transaction volumes, geographic exposure, beneficial ownership arrangements, product utilization, and corporate structure (Alessa, 2023; Wolfsberg Group, 2022). Clients consider high risk are subject to enhanced scrutiny, however, it must be acknowledged that residual risk cannot be entirely eliminated. The efficacy of a risk scoring framework is contingent upon the quality of the underlying data and the consistent application of assessment criteria. Misclassification whether by overestimating or underestimating the level of risk can precipitate adverse outcomes ranging from unwarranted financial exclusion to inadvertent facilitation of criminal activity. Accordingly, the Basel Committee (2014) underscores the necessity of technically robust models underpinned by sound governance and effective oversight.

KYC, CDD, and risk scoring are intrinsically interconnected. Deficiencies in any one of these components can compromise the effectiveness of the others. Consequently, institutions must transcend procedural compliance and embed these mechanisms within a broader organizational culture of integrity. While compliance functions are charged with the formal evaluation of regulatory adherence, their analyses depend fundamentally upon the quality of information and the cooperation of all relevant internal stakeholders. Initial client interactions, the willingness to disclose relevant structural and financial information, and the internal consistency of such disclosures may provide valuable qualitative indicators that, while not captured in standardised forms, warrant professional consideration.

Moreover, these mechanisms rarely operate under ideal conditions, their reliability depends on data quality, professional judgement, and the effectiveness of the technological tools in place, as well as the influence of internal policies and national regulations. International regulatory standards remain critical in harmonising approaches and ensuring institutions remain adaptive to evolving global threats. When implemented constructively, standardization serves not as an external imposition, but as an enabling mechanism that reinforces alignment, accountability, and resilience within an environment persistently exposed to risk.

The Rise of Artificial Intelligence in Financial Institutions

Artificial intelligence has developed from a niche research field to a transformative force across industries, including financial services (World Economic Forum, 2018). Advances in deep learning, big data, and cloud computing have enabled its adoption in areas such as transaction monitoring, risk assessments, and customer engagement (FATF, 2021). In the financial sector, AI's growing presence has generated both enthusiasm for its potential to reshape operations and caution due to the challenges of implementation. For many institutions AI is now seen as a key differentiator in a competitive and increasingly digital market (World Economic Forum, 2018).

The World Economic Forum (2018) also notes that this growth has generated a blend of optimism about benefits of AI and caution regarding its uncertainties. Such concerns have led to a relatively restrained investment approach compared to other industries, with financial institutions allocation around USD 10 billion to AI initiatives in 2020.

As the adoption of artificial intelligence continues to grow within the financial industry, traditional techniques and methods are increasingly losing relevance in favor of more innovative approaches. This process not only combines historically established practices with emerging technologies but also generates disruption that drives the creation of new procedures, risks, and opportunities. The World Economic Forum (2018) emphasizes that the capacity to strategically manage and leverage large volumes of data is expected to become a critical source of competitive advantage for those institutions able to integrate it effectively. In this regard, 76% of senior executives at the world's leading banks consider AI to be a key element of differentiation in the global market.

Applications of AI in Anti-Money Laundering (AML) Efforts

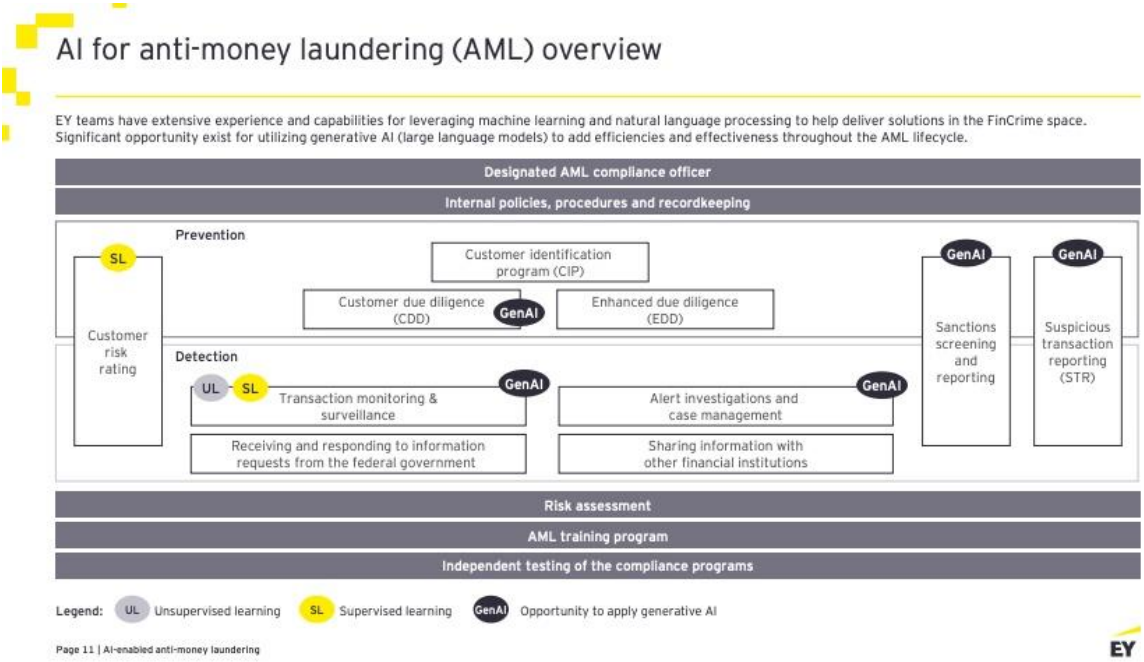
The rapid advancement of the artificial intelligence has transformed various sectors, and the financial industry has been no exception. Processes such as online banking, algorithm-driven credit scoring, and automated compliance monitoring have become integral to operations. In the context of AML, AI is increasingly recognized as a strategic enabler, strengthening core systems like Know Your Customer KYC and enhancing the efficiency of transaction monitoring (Maple, Szpruch, Epiphaniou, Staykova, Singh, Penwarden, Wen, Wang, Hariharan, and Avramovic, 2023; Digital Banking Report, 2024).

Machine learning has been particularly impactful, enabling the detection of behavioral patterns historically associated with suspicious activity, without the need for exhaustive manual configuration. By improving detection accuracy and reducing false positives, machine learning allows compliance teams to focus resources on genuinely high-risk cases. According to KPMG (2023), replacing conventional tools with machine learning models has led to improvements of up to 40% in identifying suspicious activity, while also reducing false positives. These refer to legitimate transactions that are incorrectly flagged as suspicious by detection systems, which can lead to unnecessary investigations. As highlighted by the FATF (2021), high false positive rates reduce the overall effectiveness of anti-money laundering systems by overwhelming analysts with irrelevant alerts and diverting attention from genuinely risky activity. This shift towards AI-enhanced monitoring enables institutions to allocate resources more effectively, ensuring that compliance professionals can focus on truly critical cases without compromising oversight or professional judgment.

However, their effectiveness still depends on several critical factors including data quality, proper model calibration, and their integration with human expertise. As noted by FATF (2021), machine learning should be viewed as an enabler rather than a replacement of existing frameworks. It reinforces, but does not substitute, core processes such as AML, CDD, and risk scoring.

EY (2024), illustrates how artificial intelligence, including supervised learning (SL), unsupervised learning (UL), and generative AI (GenAI), is currently being applied across the AML lifecycle. This includes customer due diligence, transaction monitoring, alert investigation and reporting processes.

Figure 2.



AI for anti-money laundering (AML) overview
Source: EY (2024). ***AI-enabled Anti-Money Laundering*****. Page 11.**

One such example is the collaboration between KPMG Belgium and DISCAI, which offers an AI-as-a-Service (AIaaS) model that provides banks with access to advanced monitoring capabilities without the need for internal infrastructure or technical management. These solutions enable behavioral pattern recognition, network analysis, and anomaly detection in an integrated and scalable way KPMG (2023).

Once machine learning tools were incorporated into regulatory compliance frameworks, it quickly became evident that training and feeding models alone would not be sufficient to meet the complex objectives of identifying illicit activity. This limitation led to the gradual integration of additional AI-driven tools, among which Natural Language Processing (NLP) that was designed to extract meaning from unstructured data including, new articles, regulatory filings, social media content, or legal documents (Flagright, 2024). NLP enhances the evaluative process by offering a broader, more extent view of customer behavior and potential third-party associations. This not only increases detection capabilities but also supports more informed decision-making across compliance teams.

One particularly compelling case, as reported by the UK-based company Ripjar (2024), involves a Tier 1 financial institution in Hong Kong, which implemented an NLP driven adverse media screening solution as part of its broader customer due diligence framework. This system was designed to enhance the prioritization of alerts by filtering duplicates, recognizing name variations, and analyzing context across multiple languages. The initiative led to a significant reduction in false positives and allowed the bank to identify potentially high-risk entities before conventional red flags were triggered.

Other particularly relevant example is the case of Danske Bank, which, in collaboration with Terada, developed a fraud detection platform combining neural networks, graph analytics, and deep learning. This initiative led to a reported 60% reduction in false positives and a 50% increase in true positive case detection, significantly improving the efficiency of internal compliance teams (Teradata, 2020).

What previously required lengthy manual investigation can now be addressed in real time, with systems capable of detecting complex patterns and uncovering relationships between entities operating across multiple jurisdictions. The ability to rapidly identify hidden structures often embedded in vast volumes of transactional data has proven particularly valuable in cross-border AML investigation, where traditional rule-based systems fall short. Moreover, by enabling a more holistic view of transactional behavior and entity relationships, graph analytics contributes the strategic depth of financial crime detection. In this sense, it represents more than just a technical innovation, it is a structural enhancement to the global AML response.

As discussed throughout previously, the application of artificial intelligence in the financial sector is not based on a single solution, but rather on a set of evolving tools that are gradually being integrated into traditional AML frameworks. The examples provided illustrated not only the variety of ways in which AI can be deployed ranging from structured data analysis to the detection of reputational risks in unstructured sources but also the global nature of the fight against financial crime. From institutions in Asia to those in Europe, Africa and America, the increasing adoption of these technologies highlights a shared recognition that money laundering is a transnational challenge requiring coordinated responses.

Although access to these tools varies among financial institutions due to economic, legal, or regulatory constraints, the shared goal remains to limit illicit transactions through more effective, data-driven systems. While AI integration into compliance processes is still in progress, evidence increasingly shows its potential to drive a more proactive, cooperative, and resilient global financial environment. Rather that replacing human expertise, AI serves a strategic enabler enhancing judgment, expending investigation, and strengthening the design of future compliance models.

Limitations of AI in AML

As part of the internal processes that banking institutions must address in their daily operations, the evaluations conducted through both internal and external audits constitute an essential activity to evaluate the quality of procedures and services the organisations provide. Hilpisch, Y. (2020) highlights the growing concern within financial institutions regarding the notion of "*explainability*", which refers to the ability to understand and substantiate the reasoning that underpins risk prediction. The author explains that artificial intelligence based on *deep learning* has the capacity to learn and adapt to the specific requirements of day-to-day operations by continuously gathering and processing the information it receives. Nevertheless, the internal mechanism of these models, built upon numerous interrelated parameters, often remains ambiguous and difficult to interpret. As a result, they become in *black box* systems that are virtually impossible to decipher and explain, even for the experts who originally developed them. This lack of transparency becomes particularly evident when audits require the institution to justify its processes and anti-money laundering measures, a situation that can lead to operational delays, reduced customer satisfaction and an increased risk of false negatives (European Banking Authority 2021).

Artificial intelligence, when applied across different industries, represents a relatively recent field that is still undergoing a process of adaptation. In the specific context of the banking sector, the gap created by its implementation in relation to internal audits has, to some extent, served as both an indicator and, control mechanism, demonstrating the extent to which this technology can currently be incorporated into anti-money laundering measures. In this regard, the use of artificial intelligence as a detection tool presents a key challenge in terms of interpreting its outputs, which has driven the development of decision tree models and model-agnostic explainability techniques such as LIME and SHAP, which aim to enhance transparency without compromising model performance. Local Interpretable Model-agnostic Explanations (LIME), works by approximating a complex model locally using simpler, interpretable models, while SHapley Additive exPlanations (SHAP), applies game theoretic principles to assign each feature a consistent contribution to the final prediction (Zafar, K., Majeed, A., Ullah, A., Shafait, F., & Mian, A. 2023). These methodologies make it possible to break down predictions into components that auditors can verify and understand. To illustrate the trade-off between interpretability and model performance, Zafar, Majeed, Ullah, Shafait, & Mian (2023) provides a helpful visual comparison of SHAP and LIME, highlighting key distinctions such as local vs. global explainability, computational cost, and treatment of feature interactions. This comparison supports the selection of explainability techniques that strike an appropriate balance between accuracy and transparency an essential feature in regulatory contexts such as AML auditing.

Figure 3.

Metrics	SHAP	LIME
Concept	Applies to the model as-is	Fits a local surrogate model to explain the complex model
Theory	Additive feature attribution based on game theory	Feature perturbation method
Type	Post-hoc model-agnostic	
Data type	Images, tabular data and signals	
Explanation	Global, local	Local
Collinearity consideration	Not in the original method	No
Non-linear decision	Depends on the used model	Incapable
Computing time	Higher	Lower
Visualization	Waterfall, Beeswarm and Summary plots	One single plot

Comparison between SHAP and LIME
Fount Zafar, Majeed, Ullah, Shafait, & Mian (2023)

Beyond model-specific explainability, there is an increasing need to adopt broader frameworks of algorithmic accountability. This involves immerse auditability into every phase of the AI lifecycle from data sourcing and model development to deployment and monitoring. Frameworks such as those proposed by Raji et al. (2020) advocate for end-to-end documentation, internal and external audits, and the development of accountability infrastructures that make decisions traceable and transparent. Such practices are critical in reinforcing trust and ensuring responsible AI use in high-stakes domains like AML.

Another limitation emerges from the strong dependence of the AI on historical data. These models are typically trained using past transactions and known typologies, which cannot reflect the current or emerging practices of money laundering networks. Criminal behaviors are constantly developing, and models based on past data may have difficulties to detect new techniques that fall outside previously identified patterns. Additionally, when training datasets are biased or incomplete due to underrepresentation of certain regions, types of customers, or transaction channels these gaps can be internalised by the systems, potentially leading to blind spots in detection (FATF, 2021) (Mehrabi et al., 2021).

Although some financial institutions report improvements on the reduction in false positives, such as Danske Bank, which achieved a decrease particularly through the adoption of more refined machine learning algorithms, others face a growing volume of alerts generated by increasingly sensitive systems. This alert overload, if not adequately managed, may overwhelm compliance teams and reduce the overall efficiency of investigations. In such context, the operational burden shifts from detecting suspicious activity to filtering through excessive signals, risking the omission of genuinely illicit behaviour due to analyst fatigue or resource limitations (EY, 2021).

Additionally, it is important to consider the unbalanced landscape of implementation. Large financial institutions may have the infrastructure and technical expertise required to deploy advanced AI systems effectively, but smaller banks or firms operating in developing economies often face significant barriers. These include not only the financial cost of adoption, but also challenges related to data availability, model governance, and regulatory readiness. As a result, the benefits of AI can be irregularly distributed, potentially deepening the gap between institutions with different levels of technological maturity (World Bank, 2022).

Furthermore, the role of human judgment in decision-making remains critical, particularly in cases where ethical or contextual considerations are involved. AI systems lack the ability to interpret social or moral dimensions, and therefore cannot fully replace human discernment in complex scenarios. An overreliance on algorithmic outputs can lead to decisions that, while technically sound, fail to account for variations that only human experience and critical thinking can evaluate.

According to The World Economic Forum (2018), artificial intelligence remains in a stage of integration with traditional methods, and this convergence is expected to gradually evolve towards greater stability, thereby enabling more effective internal processes. On the other hand, Hilpisch, Y. (2020), describes AI as an *enabler*, a facilitator that extents both human capabilities and the technological resources available within the industry. This enabling role, as noted by The World Economic Forum (2018), is closely linked to the fact that artificial intelligence is still in an early phase of adoption, during which its potential is progressively combined with existing systems.

If artificial intelligence is the new electricity, big data is the oil that powers the generators.

Kai-Fu Lee (2018)

Ethical and Regulatory Considerations

The adoption of artificial intelligence in financial institutions represent far more than a technological advancement, it signals s structural transformation that reshapes both internal processes and the way these organisations engage with their customers. Within this evolving landscape, AI-based systems challenge traditional ethical and regulatory frameworks. While the benefits in terms of efficiency and data analysis are increasingly recognized, their integration is occurring within a regulatory environment that is, at best, still catching up.

Indeed, the pace at which AI technologies advance consistently outstrips the capacity of existing regulatory structures to adapt. This regulatory lag raises a series of complex and pressing questions, particularly in high-risk sectors such as finance. Most of the current legal frameworks were conceived in an era when operations were either manual or followed fixed digital logic, and thus were never designed to address autonomous systems capable of making real-time, data-driven divisions. As the European Commission (2021) has pointed out, the absence of a harmonised legislative approach to AI has created legal uncertainty and made it increasingly difficult to ensure transparency, accountability, and effective oversight in these contexts.

Furthermore, the World Economic Forum (2020) has emphasised that the accelerating development of AI is outpacing the ability of regulatory bodies to respond, warning that current legal systems are inadequate to deal with the complexity, opacity, and velocity with which AI systems operate. This mismatch between technological innovation and regulatory capacity is not a minor administrative issue, it has concrete implications. It slows down the responsible adoption of AI and increases the risk of ethical lapses and legal exposure for institutions attempting to innovate in good faith. In the case of financial services, where trust, integrity, and legal compliance are central pillars, this gap becomes especially problematic. Without timely and coherent regulatory reform, institutions are left navigating a fragmented and outdated framework, which not only creates operational uncertainty but also undermines broader efforts to ensure that AI is developed and deployed responsibly.

One of the central tensions in the integration of artificial intelligence lies in its reliance on vast volume of personal data to train models. While such data is essential for building systems that are responsive and accurate, it also raises significant ethical and legal concerns. In the absence of robust safeguards, the processing of sensitive information can infringe upon fundamental rights such as privacy, particularly in jurisdiction with strong regulatory frameworks, such as the European Union under the General Data Protection Regulation (GDPR). Strict jurisdiction like the EU, where regulatory oversight is firmly established, play a critical role in setting clear boundaries on how far AI systems should be allowed to access and process personal information. These frameworks function not only as legal safeguard but also as ethical barriers that definer what is socially acceptable in the context of automated decision-making. However, the situation is more complex in less regulated or loosely supervised jurisdictions. In such context, AI systems may gain unrestricted access to user data, operating without clear accountability or external control. This imbalance raises serious concerns about unchecked surveillance, abuse of sensitive information, and the exacerbation of global data injustice in cross-border financial systems.

Nonetheless, regulatory adherence alone is not sufficient to address the underlying ethical complexities surrounding AI systems. There is a deeper and more pressing question about the legitimacy of constructing intelligent systems on top of data that may be reflecting social imbalance. When training datasets reflects historical inequalities or structural discrimination, AI models risk replicating and amplifying those same injustices. This concern is far from theoretical. In practice, algorithms trained on biased data can produce outcomes that systematically exclude ethnic minorities or socio-economically disadvantaged groups from accessing financial services. Such outcomes not only perpetuate inequality but also risk legitimizing algorithms forms of racism under the guise of objectivity (Barocas, S., Hardt, M. and Narayanan, A., 2019).

Recognising this, the European Commission has explicitly warned that AI, if not properly regulated, may replicate historical patterns of discrimination and further marginalise already vulnerable groups (European Commission, 2019). In particular, its ethical guidelines and proposed regulation stress the need for safeguard to prevent AI from becoming a tool that entrenches systemic bias, especially in high-risk sectors such as finance. Therefore, the deployment of AI in financial services cannot be evaluated solely on its technical accuracy or efficiency it must also be assessed on its ability to promote fairness, inclusiveness and accountability.

A parallel and equally pressing challenge arises from the lack of transparency in many AI systems, often referred to as “black boxes”. These models generate outcomes without providing a clear explanation of how decisions are reached. This opacity becomes particularly problematic in the context of anti-money laundering, where automated decisions can lead to serious consequences, including account freezes or the initiation of formal investigation. Beyond the disruption of services, such actions cast doubt on the legitimacy of the affected clients. A misclassification not only jeopardises the individual’s relationship with the institution, but also result in severe reputational damage, with financial and legal repercussions. Hence, the central issue is no longer whether AI can predict risk accurately, but whether it can do so in a manner that is transparent, traceable, and fair (Leslie, D. 2019)

Regulatory divergence across jurisdictions remains a major barrier to the ethical and effective use of AI in financial services. Laws concerning privacy, transparency, and data usage vary significantly between national and regional frameworks, creating tensions that are particularly acute in cross-border contexts. For example, in the United States, financial institutions may incorporate variables such as zip codes, credit histories, or even social media activity into risk-scoring models (Brookings Institution, 2023). In contrast, the European Union General Data Protection Regulation (GDPR) imposes stricter data minimisation and purpose limitation requirements, potentially prohibiting the same practices if they result in indirect profiling (European Commission, 2021). While U.S. regulation often adopts a sector-based or self-regulatory approach, the EU mandates formal justification, human oversight, and the right to explanation under Article 22. This lack of alignment means that an AI-driven decision could be lawful in one jurisdiction and unlawful in another. As the World Economic Forum (2019) notes, this inconsistency undermines legal predictability and complicates compliance across interconnected financial systems. Without enhanced global coordination, building AI systems that are universally ethical, transparent, and enforceable will remain a significant challenge.

In response to these challenges, a range of conceptual frameworks and governance practices have emerged to promote a more balanced relationship between technological innovation and ethical responsibility. One of the most prominent is the Ethics-by-design approach, which advocates for an integration of core ethical values such as transparency, non-discrimination, and respect for fundamental rights into the early stages of systems development. Crucially, embedding these principles from the outset allows organisations to anticipate and prevent ethical risk before they materialise, rather than attempting to rectify harm after it has already occurred (Taofeek, A. 2025)

On the other hand, the Human-in-the-Loop model offers a complementary safeguard, arguing that critical decision particularly those with legal, reputational or financial consequences must remain under meaningful human supervision. While AI can undoubtedly support compliance team by improving detection and reducing operational burdens, it cannot and should not replace human judgement. The capacity of experienced professionals to interpret delicate contexts, apply intuition, and assess significance remain essential. In this sense, human oversight is not a formality but necessary ethical counterbalance to the inherent limitation of algorithmic reasoning (Taofeek, A. 2025).

In this context, the use of audit trails becomes essential for ensuring accountability and institutional transparency. By documenting each stage of an AI system's decision-making process including data sources, model development, updates, and human oversight these traceable records enable both internal and external audits. They serve not only as a tool for retrospective evaluation but also as a proactive mechanism to reinforce compliance and minimise ethical risk. Equally relevant are regulatory sandboxes, which provide controlled environments where AI applications can be tested under supervisory scrutiny before full-scale deployment. These mechanisms allow institutions to identify flaws, correct biases, and validate outcomes without exposing the financial system or individual rights to undue harm. Such adaptive spaces reflect a broader understanding that regulation, much like the technology it governs, must be capable of evolving. Given that AI systems are in continuous deployment, regulatory frameworks cannot remain static. Instead, there is a need for a new phase of governance one that balances baseline standards with flexible, forward-looking oversight capable of adapting to technological shifts (Taofeek, A. 2025).

Ultimately, addressing the ethical and regulatory complexity of AI in AML requires a collective and inclusive approach. It is no longer sufficient for developers to meet technical specifications or for regulators to enforce isolated limits. Rather, ongoing collaboration between technologists, policymakers, civil society, and ethicists is imperative. More importantly, this cooperation must extent beyond national borders. Money laundering is a transnational crime with consequences that directly or indirectly affect entire societies. Therefore, regulatory responses must also be multilateral. Only through shared standards and coordinated global efforts can the integrity, legitimacy, and fairness of AI systems in financial surveillance be truly secured. Framing ethical AI within this global context not only reinforces fundamental values, but also positions it as a long-term strategic investment one that strengthens regulatory stability, institutional trust, and reputational resilience.

Summary and Conclusion of the Literature Review

Globalisation has acted as a key enabler in the fight against money laundering by fostering financial market interconnection, accelerating cross-border information exchange, and promoting the adoption of shared international standard (World Bank, 2022). This interconnectedness has allowed international bodies such as the FATF, INTERPOL, and the World Bank to coordinate strategies, disseminate knowledge, and provide technical assistance to jurisdiction with fewer resources. Nevertheless, these organisations face persistent challenges, including economic disparities between countries and differences in legal frameworks, which create operational asymmetries. Such gaps are actively exploited by criminal networks to move illicit funds into jurisdiction with weaker oversight (UNODC,2023). In addition, these entities must alight their actions with human rights and privacy regulations, ensuring that anti-money laundering measures are grounded in universal principles. Despite these complexities, the collective objective remains clear: to detect, reduce, and prevent illicit operations seeking to infiltrate local and global financial systems. Achieving this requires genuine international cooperation that transcend political, religious, or economic differences, prioritizing the protection of the integrity of the financial system.

Within this evolving landscape, AI has entered the financial sector as a disruptive force, reshaping processes and compliance approaches. In a context where millions of transactions occur daily, human capacity alone struggle to detect and intercept illicit activity with sufficient speed and accuracy. AI functions as a strategic enable, but its deployment must be supported by a full understanding of its operations, capabilities, and limitations. Key risks include biases embedded in historical datasets, uneven technological access among institutions, and explainability challenges that can undermine trust and operational effectiveness (FATF, 2021; European Banking Authority, 2021). Transparency and accountability in AI systems are therefore critical to ensuring that these tools strengthen, rather that weaken, compliance frameworks.

The synergy between human and artificial capabilities offers significant potential. AI contributes systematic processing and scale, while human expertise brings contextual judgement, ethical reasoning, and adaptive decision-making. The human role extents beyond supervising AI outputs to actively training models, embedding institutional knowledge, and ensuring that decisions align with broader social and ethical standards (Taofeek, 2025). In this sense, society as a hole becomes the ultimate beneficiary. This study positions AI not as a replacement for human work but as a force multiplier expanding the capacity of financial institutions to anticipate risks, enhance resilience, and reinforce the global fight against money laundering.

CHAPTER 3 - METHODOLOGY

This section outlines the research methodology adopted to address the central research question and achieve the stated objectives. It explains the rationale behind the chosen approach, the design of the study, and the specific methods used for data collection and analysis. The methodology has been developed to ensure alignment with the scope and purpose of the research, supporting a careful and in-depth exploration of the key challenges in AML and the role of AI as both an enabler and a potential threat within AML frameworks. The chapter methodology also reflects on alternative methodological options considered, provides the justification for the selected approach, and outlines the measures taken to maintain the credibility, dependability, and ethical integrity of the research process.

Research Design

The study adopts a qualitative research design, as this approach is well suited to exploring multifaceted issues within real-world context, such as the challenges financial institutions face in anti-money laundering and the role of AI within these frameworks. A qualitative approach enables the collection of rich, detailed accounts that can capture the nuances of professionals experience and institutional. Practices. structured interviews were selected as the primary method for gathering first-hand perspectives from professionals with direct involvement in compliance, risk management, or technology roles within financial institutions. This method provides flexibility to explore key themes while allowing participants to elaborate on issues most relevant to their expertise. The qualitative findings are supported by a review of relevant academic studies and industry reports, which helps place the participants experiences in the wider context of global AML regulations, technological developments, and organizational practices. Alternative approaches, such as quantitative surveys or mixed-methods designs, were considered, however, they were not selected because the qualitative approach allows for a richer understanding of participants perspectives capturing the human dimension of their experiences in a way that purely numerical data could not.

Sample Selection

The investigation involved seven structured interviews with banking professionals representing a range of departments, including compliance, risk management, treasury back office, and portfolio management in foreign exchange. This diversity was intentionally selected to capture variations in how AI and AML are perceived and implemented across different operations context. The focus on departments directly involved in compliance processes and day-to-day risk management rather than on the technical implementation of systems. This approach recognizes that certain departments area classified as higher risk for money laundering by international regulatory bodies such as the Financial Action Task Force (FATF, 2021). For example, foreign exchange operations are often subject to stricter compliance measures than standard retail banking activities, such as account openings without foreign currency transactions.

Participants had between five and over thirty-five years of experience in the financial sector, with ages ranging from their early thirties to mid-sixties. While the majority occupied management or decision-making positions, the sample also included professionals involved in operational processes, ensuring representation of both strategic oversight and frontline practice. The inclusion criteria required a minimum of five years' experience in the financial industry, with preference given to individuals whose roles allowed them to contribute insights into AML practices from either a managerial or operational standpoint. No participants were excluded once the defined target profile had been established.

This sample was considered appropriate for the research because it prioritises the operational and human aspects of AML practices, aligning with the study's view that while AI can be a valuable tool, it cannot fully replace human judgment and expertise. The selection strategy was therefore directly aligned with the study's aim to integrate practical insights into a broader understanding of global AML and AI challenges. Participants were accessed through professional networks, including contacts from previews employment and personal connections across different regions. This approach ensured the recruitment of individuals with relevant expertise and varied professional contexts, thereby enriching the depth and breadth of the data collected.

Research Instrument

Structured interviews were used as the primary research instrument in this study. The interview guide was designed to address the central research question by exploring operational, strategic, regulatory, ethical, technological, and human dimensions of AML and the role of AI within these frameworks. The design of the guide followed established best practices for qualitative interviewing in social sciences and management research, ensuring clarity, neutrality, and logical sequencing of topics (Kallio, H., Pietilä, A.-M., Johnson, M. & Kangasniemi, M. 2016). Questions were organised to move from broad, general prompts to more specific inquiries, creating a natural flow that encouraged participants to share detailed experiences before addressing more sensitive or technical aspects.

The questions were derived from insights gained in the literature review, ensuring direct alignment with the research objectives and allowing for a balance between comparability across participants and the depth needed to capture individual perspectives. For instance, the recurring challenge of global regulatory fragmentation highlighted in previews studies (FATF, 2021; Basel Committee, 2017) informed one of the core questions, which seek to understand how this fragmentation affects the effectiveness of AML systems from the participants perspective. Similarly, the review of reports discussing the risks of predisposition and inequality in the use of AI within financial environments (Mehrabi et al., 2021) prompted the inclusion of a question aimed at exploring participants views on fairness and the ethical implications of AI adoption in AML.

Each question was linked to one or more of the study's objectives to ensure purposeful data collection:

- Question 1-3 aimed to identify operational and regulatory challenges.
- Question 4-7 explored the perceived benefits and risk of AI in AML.
- Question 8-10 examined the ethical consideration, and potential consequences in AI in AML.
-

Data Collection

Initial contact with participants was established in April 2025 via email to explain the purpose and scope of the research. Formal interviews sessions were then scheduled between May and June 2025, using virtual meeting platforms such as Zoom. This format was chosen to enable participation across different geographical locations while ensuring privacy for a sensitive topic such as AML.

At the start of each session, the researcher introduced the study, explained the voluntary nature of participation, and provided assurances of confidentiality and anonymity. Explicit informed consent was obtained from all participants before beginning the interview. In total seven interviews were conducted.

Each interview lasted approximately 45 to 60 minutes, and it contained 10 core questions, supplemented by follow-up prompts to clarify responses and explore emerging themes when relevant. While a formal pilot interview was not conducted, the guide was internally reviewed against academic and industry sources to ensure conceptual clarity, alignment with the research question, and avoidance of leading or overly complex wording. This format allowed participants to share experiences and insights while maintaining a consistent structure across all interviews, facilitating thematic comparison in the analysis phase.

Data Analysis

The interview data were examined using thematic analysis, following the approach outlined by Braun, V. & Clarke, V. (2006). This method was chosen because it offered the flexibility to explore both themes anticipated from the literature review and new perspectives that emerged directly from participants experiences. It was particularly suited to this study's aim of understanding the operational, human, and regulatory aspects of AML in relation to AI.

The analysis began with several close reading of each transcript to gain familiarity with the content and context of each interview. During this process, I noted initial ideas and observations, which were then organised into preliminary codes capturing key concepts and recurring issues. These codes were reviewed and grouped into broader categories, forming themes that reflected patterns across different participants while preserving the variation of individual viewpoints. In developing and refining these themes, particular attention was paid to contextual factors such as participants years of experience, generational differences within the sample, and the specific roles they held in the financial industry, as these elements often shaped not only how they responded to the integration of AI in AML processes, but also the way they carried out their responsibilities, their direct interaction with core areas such as compliance, and the influence of their personal ethics and professional development within the institutions.

The process was carried out manually without the use of specialist software, allowing for sustained engagement with the material. This hands-on-approach supported a deeper interpretation of the data and made it possible to integrate the interview findings with relevant insights from the literature review, strengthening the connections between participants perspectives and the broader global discussion on AML and AI.

Ethical Considerations

This research was conducted in accordance with the ethical guidelines of the National College of Ireland. All participants were provided with an informed consent form outlining the purpose of the research, the voluntary nature of the participation, and the measures taken to protect their confidentiality and anonymity. Consent was obtained in writing via email before any interview took place.

To ensure anonymity, no names, place of work, institutional identifiers, or other personally identifiable information were recorded in the transcripts or the final report. Participants are referred to using generic role descriptions, such as "Compliance Officer" or "Banking

Professional”. Interviews were audio-recorded without video, stored securely in encrypted files, and will be permanently deleted upon completion of the academic evaluation process.
Given the sensitivity of the subject matter, care was taken to frame questions in a way that avoided soliciting any confidential client information or breaching organizational policies. Some individuals declined to participate in the interviews due to the sensitive nature of AML related topics, and the decision was respected in full. Participants were reminded that they could skip any questions or withdraw from the study at any time without consequences.

Limitations of Methodology

While the methodology was designed to address the research question effectively, certain limitations specific to the AML and AI context should be acknowledged. The study was based on seven interviews, which, although sufficient for generating in-depth qualitative insights, cannot capture the full range of perspectives present across the diverse global AML landscape. The participants professional backgrounds, offered valuable diversity, but their viewpoints remain influenced by the regulatory and organisational contexts in which they operate.
The sample did not include professionals from IT departments, a deliberate methodological choice to focus on operational and compliance perspective. This allowed for an exploration of the human and procedural aspects of AI adoption in AML, but also means the study does not provide direct insights into the technical development and integration of AI tools. Additionally, due to the sensitive nature of AML-related topics, some potential participants declined to be interviewed, which may have reduced the breadth of viewpoints, particularly from individuals working in higher-risk operational areas.
All interviews were conducted virtually, while this format facilitates access to participants in different regions, it may have limited the observation of non-verbal signals that can sometimes provide additional context to verbal responses. Furthermore, five interviews were conducted in Spanish and two in English, requiring translation for the research purposes. Although care was taken to ensure accuracy, subtle difference in language could have affected the interpretation of meaning, especially when discussing technical compliance terminology or culturally specific understanding of AML risks.
Despite these limitations, the chosen methodology was well suited to capturing the nuanced, experience-based perspectives necessary to explore the operational realities and ethical considerations of AI adoption within AML frameworks.

CHAPTER 4 – FINDING

This section presents and analyses the findings of the study, examining how they align with, and in some cases differ from, the literature reviewed earlier. Rather than offering a purely descriptive inventory of results, the analysis identifies patterns, contrasts points of convergence and divergence with prior research, and provides an initial interpretation of their significance for the application of AI to AML.

Within this context, the findings are organised into three interlocking thematic areas that reflect both the challenges and opportunities highlighted in the literature. First, operational and regulatory challenges remain a persistent constraint for financial institutions, which must navigate the complexity of the offence, fragmented legal frameworks, and continuous compliance pressures (Levi, M. & Reuter, P., 2006; Unger & Van der Linde, 2013). Secondly, the data reflect perceptions of the benefits and risks of AI within AML processes, consistent with KPMG (2023): while AI can strengthen detection and efficiency, its deployment raises concerns about model opacity, algorithmic unfairness, and data limitation, issues that condition its actual value unless addressed through strong internal controls and oversight. Finally, the findings highlight the human role, ethical considerations, and potential risks of algorithmic unfairness in AI adoption, which the literature frames as central to ensuring transparency, accountability and fairness in high-risk settings (European Commission, 2019; Barocas, S., Hardt, M. and Narayanan, A., 2019).

Each section integrates the most salient evidence with an initial, theory-informed interpretation of its implications. A thematic analysis was conducted to identify common patterns and trends, as well as notable divergences across participants. The organisation into thematic blocks follows the categories defined in the methodology section to preserve consistency and interpretive clarity, beginning with an examination of the operational and regulatory challenges that influence the capacity of financial institutions to implement AI in AML frameworks.

Operational and Regulatory Challenges

The interviews conducted reveal that, by the very nature of AML, operational and regulatory challenges are not incidental but implicit to the process. These challenges operate at two interconnected levels: internally within each financial institution, and externally as part of the wider financial ecosystem, both domestically and globally. Together, they set the boundaries and in some cases the constraints on what financial institutions can realistically achieve when integrating AI into their AML framework. The literature identifies a set of persistent and clearly defined challenges in AML, including the transition with the old systems to the new, the diversity of regulatory frameworks, and the operational challenges caused by limited resources and coordination gaps (Levi, M. & Reuter, P., 2006; Unger & Van der Linde, 2013). The interviews reveal these issues and illustrate their practical consequences in daily operations. Participants described how fragmented monitoring tools and databases disrupt workflow continuity, prevent AI from working with complete datasets, and slow down decision-making processes. They also emphasised that these challenges are not static, their impact is shaped by institutional culture, uneven resource allocation, and the degree of cross-departmental collaboration. The findings indicate that these challenges extent beyond purely regulatory or technological consideration, reflecting deeper organisational dynamic within individual institutions and systemic operational patterns across the ecosystem banking sector.

A significant issue highlighted in the interviews was the overload of alerts combined with insufficient time for thorough review. Although the FATF (2021) notes that high false-positive rates place a substantial burden on analyst, the participants introduced a crucial operational perspective: the ongoing pressure to *"clear the queue"* of cases frequently results in expedited and superficial assessments. Such sustained operational strain not only compromise the quality of human decision-making but may also introduce unreliable examples into AI models, progressively dismissing their accuracy and, over time, undermining the confidence of compliance offices in the systems they are required to use.

Beyond its technical implications, these persistent alerts overload also exposes weaknesses in the collaborative culture within financial institutions. Several participants referred to internal operational barriers that hinder effective collaboration. While the literature often emphasises technological integration, the interviews underscored that interdepartmental cooperation does not always flow smoothly in practice. Without coordinated efforts and a shared understanding of risk across units, advanced tools are at risk of being underutilised or misapplied. This observation reinforces Levi, M. & Reuter, P. (2006) argument that operational resilience depends as much on organisational culture as it does on technical infrastructure.

Building on the earlier point about the lack of integration within internal systems, participants stressed that the issue is not only technical organisational: monitoring tools, client databases, risk-assessment platforms, and even interbank interfaces often operate in silos, preventing a consolidate view of information. As one interviewer observed, *"each system works on its own,* *the information exists, but you have to look in five different places to see the full picture".* This is consistent with prior assessment that treat poor integration as a core vulnerability (FATF, 2021; Europol, 2021). Crucially, when AI is deployed into landscape it inherits these divisions, resulting in partial inputs, incomplete analyses, and weaker pattern detection thereby constraining model performance and slowing compliance decision-making.

This challenge becomes even more complex in cross-border operations. Participants with international exposure describe regulatory divergence as a major brake on effectiveness: before an AI system can process multi-jurisdictional data, it often must be "translated" and adapted to the source country's format and criteria. For instance, some jurisdictions record only one surname while others require two family names, a mismatch that can produce spurious hits on sanctions or watchlist without any underlying risk. This additional verification destroys timeliness and reduces the value of real-time monitoring. In parallel, legal constraints on cross-border data sharing well documented in the literature (FATF, 2013; World Bank, 2018) not only impede investigations but also shape training data, leading to models that are over-fitted to specific regulatory context and less portable elsewhere (Unger & Van der Linde, 2013; World Bank, 2018). While several institutions view AI as a strategy for internal standardisation of risk assessment, the interviews suggest that absent greater regulatory harmonisation, these gains remain largely confined within the firm.

Overall, the findings show that operational limitation and regulatory misalignment frame the environment in which AI must operate in AML. Understanding these constraints is essential and provides the basis for examining the potential benefits and risks that such technologies may bring.

Benefits and Risks of AI in AML

With these constraints in mind the interviews revealed that AI in AML is perceived through a dual lens: on one hand, as a tool that can significantly enhance detection and investigation efficiency, on the other, as a source of new risks that require close oversight. Participants described clear gains in speed, accuracy, and the ability to bring together large volume of information, but also pointed to ethical, organisational, and technical concerns when AI is relied on excessive or insufficiently supervised. These perceptions align with the literature's recognition of AI as both an enabler and a potential threat in financial crime prevention, while also offering practical insight into how these dynamics play out in day-to-day AML operations.

Risk

Participants warned that excessive reliance on AI can gradually erode human analytical skills. An observation consistent with FATF's emphasis on the primacy of human judgement and with Barocas, S., Hardt, M. and Narayanan, A. (2019) concerns about decision quality in high-stakes settings (FATF, 2021; Barocas, S., Hardt, M. and Narayanan, A., 2019). Moreover, several highlighted the risk of "*blind automation";* systems operating without sustained human-in-the-loop oversight (Taofeek, 2025), which encourage closed decision environments and amplifies bias. This is consistent with the European Banking Authority's warning on black-box models complex systems whose inner working are unclear even to developers and often require auxiliary tools to understand it, underscoring that, without human supervision, AI in AML can introduce material risk, as one interviewee put it, "*there are processes where the system decide, but we cannot explain how it reached that conclusion".* Another added, "*the tool may be very accurate, but if we do not understand the logic behind it, we cannot fully trust results."* In practice, such opacity not only limits accountability but also opens the door to uses beyond the original intent, as the European Commission (2019) mentioned.

Benefits

Among the benefits most frequently cited by participants was AI's ability to access and analyse large volumes of information in very short timeframes, including from open-source data, and to produce compilations, comparisons, and concise summaries that support investigation. As one interviewee described, *"analysis of open-source information on the web in seconds, instants comparative data compilation, and the creation of relevant summaries and graphics."* This reflects FATF's (2021), observations on the speed and precision such technology can offer. Several participants also reported improvements in investigate effectiveness and in detecting unusual operations, particularly when alerts were aligned with specific regulatory requirements. One noted, *"detect unusual operations and suspicious transaction more promptly and accurately, raising alerts in line with laws and regulatory bodies."* Others emphasised AI's role prioritising operations with higher probability of non-compliance, enabling teams to focus resources on the most critical cases, an approach consistent with KPMG's (2023) findings on optimising AML workflows. On AI's capacity to keep pace with complex transnational laundering schemes, opinions were divided: some highlighted adaptability and predictive capability, while others cautioned that it still requires constant updates and cannot substitute human judgment. As one participant mentioned. "*AI can anticipate, but it does not understand the context like a person does."* This perspective aligns with literature framing AI as an enabler rather than a complete replacement for human supervision in AML (FATF, 2021; Hilpisch, Y., 2020).

Overall, the evidence suggests that while AI offers a clear gain in efficiency and precision within AML, its real value depends on sustained human management and strong regulatory and organisational safeguards. This sets the stage for examining the human role, ethical responsibilities, and the risk of algorithmic imbalances in high-stakes financial decision-making.

Ethical Safeguards, Fairness and the Future of Human–AI Collaboration in AML

In AML, the integration of AI is not solely a technological shift but a human and ethical one. The interviews show that fairness, transparency, and accountability are experienced as practical challenges with direct consequences for trust in automated systems. Participants emphasised the need for clear safeguards, the prevention of structural inequities, and a well-defined balance between human judgement and machine capability. These perceptions not only align with international principles but also highlight operational realities what will shape the next stage of human-AI collaboration in terms of AML.

Ethical risks and fairness

Interviews indicate that fairness concerns appear not only from model quality but also from internal choices within institutions. Participants pointed to three drivers: reliance on historical data - *"the system detect a new patter until it looks like something it has seen before"*- which delays recognition of emerging typologies (FATF, 2021; Mehrabi et al., 2021), design errors that misclassify legitimate activity, as one mentioned "*it can flag a legitimate transaction as suspicious just because it resembles a previews case".* Echoing concerns on representativeness and discrimination (Barocas, S., Hardt, M. and Narayanan, A., 2019; European Commission, 2019), and organisational decision that prioritise AI spend over analyst training. Notably, this last point extents the literature: while prior work often focuses on disparities between institutions (World Bank, 2022), interviewees emphasised inequities within a single firm when teams lack the skills to challenge model outputs. The result is a higher risk of uneven or discriminatory risk assessment. Thus, the evidence partly aligns with the literature's principles on fairness and transparency, but it also surfaces operational dynamics budget trade-offs and capability gaps that determine whether those principles hold in practice.

Participants also identified what they saw as essential conditions for the responsible use of AI in AML: specialised training for those operating the systems, clear rule on data confidentiality, ethical codes with explicit limits on automated actions, and, notably, a unified global framework requiring transparency in the criteria used by each model. These points align with the principles set out by the European Commission (2019) and FATF (2021) on transparency, accountability, and governance, yet go further by framing the lack of an enforceable global standard as an operational gap that directly affects day-to-day AML work.

Interviewees often envisioned a gradual shift towards what several described as a "50-50" balance, in which AI speeds up risk prioritisation and detection while the final authority remains with human analysts. Ongoing training was seen as essential to sustain this balance, ensuring teams can both leverage critically evaluate automated outputs. Some participants also pointed to the value of closer cooperations between regulators and industry not only to harmonise technical standard but to immerse ethical considerations directly into the design and deployment of AI tools. This forward-looking perspective closes the discussion on fairness and safeguards, highlighting that the future of AML will depend as much on collaborative governance as on technological capability.

CHAPTER 5 - DISCUSSION

The discussion chapter builds on the previous analysis by moving from describing the results to interpreting what they mean in a broader context. It considers how the findings align with or diverge from existing research, and what they reveal about the realities of integrating AI into AML beyond its technical capabilities. It also reflects on what these findings imply for daily practice, long-term strategy, and international coordination, connecting the lived experiences of AML professionals with the wider policy and governance debates.

The findings of this study confirm that, while operational and regulatory barriers described by Levi, M. & Reuter, P. (2006), Unger & Van der Linde (2013) and the FATF (2021) remain a significant challenge, the persistence of these barriers shows that technological tools alone cannot fully address structural inefficiencies or inconsistent enforcement. The real strength behind effective anti-money laundering measures lies not only in technology or regulations, but in the people who operate the system. The literature acknowledges the role of compliance officer (Buchalter, 2022) and the value of training, yet often treats these as supporting elements to technical and regulatory processes. The interviews suggest otherwise: skilled and well-supported staff are not simply an accessory to the system; they are the main driver of whether AI is applied successfully in AML. Organisational culture acts as a complementary force that enables them to work with consistency, collaboration, and purpose, shaping how rules are applied, how technology is integrated, and how emerging risk are addressed.

Financial institutions, in this sense resemble a living organism. The people working within them are the heart that drives commitment, cooperation, and constant scrutiny, regulations are the veins that channel this flow within a safe framework, and the information moving through AML processes is the blood that sustains the systems. AI, in this analogy, acts as a pacemaker; it can optimise rhythm, detect irregularities, and improve data circulation, but its impact depends on a strong heart and clear veins. While much of the reviewed literature-including the sources examined in this study-focuses primarily on AI's technical capabilities-such as reducing false positives or speeding up analysis- this research highlights that without a strong *"human core,"* those capabilities will not deliver their full potential. This reflects a gap in existing studies, where the human and cultural dimensions of AML work are often underexplored.

The interviews show that the value and performance of AI in AML are not universal. Its effectiveness depends largely on context: available infrastructure, data quality, regulatory frameworks, and-above all- the ability of people to adapt and apply judgement. This aligns with FATF (2013) and the World Bank (2018), which note that developing economies face heavier regulatory and operational burdens, and with Unger & Van der Linde (2013), who highlight how regulatory fragmentation limits cross-border effectiveness. Participants, however, added that this variability is not always a disadvantage, in some cases, it can encourage creative problem-solving and more adaptable solutions than those found in rigidly standardised systems. Participants acknowledged that the global financial system understands achieving full standardisation across jurisdictions is unrealistic, difference in capacity, priorities, and resources mean that complete alignment is either a very long-term goal or one that may never be fully realised. Yet, despite these limitation, international bodies continue to push for greater harmonisation, recognising that even partial progress can improve cooperation and detection. Financial institutions do not operate in identical environments, alongside meeting regulatory requirements, they are also competitive businesses. This does not mean opening the door to illicit activity, but rather that, even within regulatory boundaries, they seek to differentiate themselves and find competitive advantages. Such flexibility allows them to adapt processes to their operational realities. In lower-resource contexts, participants described this adaptability as *"a matter of survival,"* enabling institutions to sustain AML effectiveness by tailoring methods to local realities instead of depending entirely on a one-size-fits-all technological approach. For instance, participants cited examples from smaller banks operating in developing economies, manual review layers or hybrid systems combining basic automation with human-led verification often perform better than importing complex AI platforms designed for high-resource environments.

The findings also reveal significant tensions when the balance between human oversight and technological capability is not well managed. Several participants described cases of "blind automation", where excessive reliance on AI outputs replaced critical analysis. This approach can amplify existing biases in the data and, over time, erode the analytical skills of staff. As noted in the interviews, when analysts stop questioning the results and simply validate them mechanically, the ability to detect new patterns or inconsistencies outside the trained models is lost. This aligns concerns raised by Barocas, S., Hardt, M. and Narayanan, A. (2019) that over-automation can give a false sense of objectivity, masking bias and weakening the system's ability to adapt to unfamiliar threats.

A central aspect of this tension is the opacity of complex black box systems used in some AI applications. This aligns with Hilpisch, Y. (2020) discussion of *explainability*, understood as the ability to explain and justify a model's decisions. In the context of AML, where-as highlighted in the literature-the financial sector plays a central role, operating in practice much like a for of financial law enforcement with the responsibility to detect, prevent, and report illicit activity, the lack of explainability poses a significant reputational risk. Institutions therefore face an additional challenge: introducing new technologies that enhance efficiency without encouraging blind trust in them. As reflected in several interviews, there is a need to communicate to actively remind staff that a powerful tool still requires their own judgement. Striking that balance, especially under constant pressure to process alerts quickly, can be a difficult balance to achieve in practice. Although the concept of regulatory sandboxes mentioned by Taofeek, A. (2025) was not explicitly referenced by most of the participants, the importance they placed on being able to review and challenge AI-generated alerts points in a similar direction. Having clear accessible records of how an alert was triggered was seen as essential for maintaining both trust and accountability in the process, echoing the role that sandboxes and other controlled testing environments can play in refining AI tools before full deployment.

Beyond its technical impact, integrating AI into AML processes brings ethical and strategic questions that go well beyond operational efficiency. As the European Commission (2019) notes, the way this technology is designed, implemented, and monitored will shape not only its detection capabilities but also public perception of fairness and the legitimacy of the financial system. If AI is seen as biased, opaque, or applied inconsistently, it can undermine public trust and weaken the sector's role in safeguarding financial integrity, a concern also raised by the FATF (2021). Many of the points raised in interviews align with the principles of "Ethics-by-design"-building ethical safeguards into AI from the start-and "human-in-the-loop"-where human review is a formal, ongoing part of the workflow. Rooting these into institutional practice could help ensure the balanced oversight participants felt was essential. Participants also pointed to earlier technology rollouts in other compliance areas where poor communications and unclear lines of responsibility caused trust issues among both staff and customer, showing that these risks are not theoretical.

Avoiding these risks requires a shared commitment from financial institutions, regulators, and international bodies to ensure that innovation does not unintentionally create new forms of exclusion or inequality. The World Bank (2018) warns that the absence of coherent global frameworks leads to fragmented adoption and persistent disparities. This study's findings confirm that such gaps are visible in everyday AML operations, particularly in cross-border cooperations within institutions operating under resource constraints. For practitioners, AI should not be valued solely for its speed or efficiency, but for its potential to strengthen cooperation and transparency both within institutions and across borders. Only a small number of participants explicitly linked AML measures to broader social outcomes, such as preventing the financing of human trafficking, drug trade, or systemic corruption. However, this perspective highlights an important point: AML is not solely about stopping illicit funds from entering the financial ecosystem, but also about reducing the social harms these funds enable. NASDAQ (2024) reports that the financial flows generated by these crimes reach staggering levels globally, underscoring the scale of the challenge and the potential impact of effective

AML measures. Embedding this awareness into compliance culture could strengthen both the ethical foundation and the operational commitment to AML objectives.

This approach, placing ethics and governance on an equal footing with innovation, offers a pathway for the responsible use of AI in AML. As this study suggest, its future will depend not only on technical progress but on the commitment of all stakeholders to balance efficiency, equity, and trust, ensuring that technology strengthens, rather than undermines, the integrity of the global financial system. As one interviewee observed, *“The bank is by nature, a planning-oriented institution with strategic outlook, and this philosophy will be no exception in the case of AI. Its integration will be gradual, with careful evaluation of how it aligns with the bank's operational needs and of course, with, AML regulations.”* This step-by-step approach captures the broader conclusion emerging from this study: AI in AML will only reach its full potential when technological innovation, human judgement, and ethically grounded oversight are developed together, each reinforcing the others rather than competing for priority.

“Technology is neither good nor bad, but humans make it so”

(Kranzberg, 1986).

CHAPTER 6 – CONCLUSION

This study has addressed the central research question concerning the key challenges faced by financial institutions in the global fight against money laundering, and the extent to which artificial intelligence can operate both as an enabler and a potential threat to strengthening prevention frameworks.

The findings confirm that operational and regulatory challenges are structural rather than incidental. Fragmented legal frameworks, limited international cooperation, alert overload, and the lack of system integration continue to constrain the effectiveness of anti-money laundering measures even in well-resourced institutions. These barriers, already identified in the literature (Levi & Reuter, 2006; FATF, 2021; World Bank, 2018), were validated and expanded in practice: the daily pressure on compliance teams, internal frictions between departments, and disparities in institutional capacity across jurisdictions indicate that these obstacles cannot be resolved through technology alone. The interviews also underscored that these issues are embedded within organisational cultures, influencing how tools are used, how risk is prioritised, and how collaboration is fostered or hindered.

Within this context, AI emerges as a powerful enabler with significant potential to optimise detection, prioritise risks, and reduce false positives. Machine learning models, natural language processing, and network analytics have demonstrated measurable benefits, such as improved identification of suspicious patterns and more effective alert prioritisation (Ripjar, 2024). However, its actual impact depends on factors that extent beyond the technical domain: the quality and representativeness of the data, the ability to audit and explain algorithmic decisions, and the integration of these tools into an organisational culture that values human oversight. The most tangible benefits are realised when AI complements, rather that replaces, professional expertise, reinforcing the ability to respond to complex and adaptive criminal typologies that evolve rapidly in the global financial system.

At the same time, the research shows that AI can become a source of risk if implemented without adequate safeguards. The opacity of certain models, an excessive dependence on historical data that may fail to capture emerging laundering methods, and unequal access to the technological infrastructure needed for deployment can amplify biases, create a false sense of security, and-at worst-undermine both internal and external confidence in prevention systems. These risks are not merely theoretical, evidence from the interviews shows that when automated decision are left unchallenged, operational accuracy and institutional legitimacy can be compromised, echoing the caution raised in earlier studies on “black box” models and algorithmic accountability (Hilpisch, 2020; Barocas, Hardt & Narayanan, 2019).

Regarding the literature, important gaps were identified. While numerous studies document the technical advantages of AI in AML (FATF, 2021), aspects such as organisational culture, internal collaboration dynamics, and the ethical implications of AI adoption were not a central focus on this research. Although these elements emerged as relevant from the interviews, their in—depth examination would require future studies designed to address them explicitly and systematically. Furthermore, the scope of the interviews and the qualitative nature of the sample mean that the result should be interpreted with caution and not generalised without additional research to broaden the evidence base, ideally through comparative studies across jurisdictions and institutional types.

In sum, the hypothesis is only partially confirmed: AI has the potential to be a key enabler for strengthening AML frameworks, but its contributions is contingent upon the robustness of the human, regulatory, and ethical environment into which it is introduced. Equally, it can become a threat if deployed without transparency, critical oversight, and regulatory frameworks that evolve alongside technological change. The evidence suggests that the most resilient AML strategies will be those that integrate AI into a human-led decision-making process, ensuring that technology amplifies, rather than decline, ethical responsibility and contextual judgement.

Personal Reflections on the Study

When I began this research, I expected to show how AI could be embedded into banking institutions as a fully fortified and almost impenetrable defence against money laundering-one that might relieve human teams of the risk of error in detecting illicit operations. Early in the study, the definition of money laundering put forward by the Bank for International Settlements stood out to me. It did not just describe the process itself, but highlighted the human factor as central to prevention. Initially, I envisioned this project would chart the beginning of a complete integration of AI into AML measures, supported by promising results in the literature that confirmed the strong performance and tangible gains from such technologies.

However, as the research progressed, my perspective shifted. AI in AML is not solely about efficiency or speed-it is fundamentally about the people who operate these systems. The technology can be trained, it does not tire, and it can process volumes of information beyond any human capacity. Yet, despite these advantages, human judgement, creativity, and intuition remain irreplaceable. The professionals in AML teams are not simply end users, they are the ones who guide, challenge, and shape the technology to ensure it align with ethical, regulatory, and operational realities.

There is no doubt that banks will face increasingly complex AML challenges in the years ahead. Beyond any technical advantages, the real test will be ensuring that AI remains a facilitator rather than a substitute. Based on the evidence gathered in this research, I conclude that AI's role in AML frameworks is best understood as a powerful ally rather than an inevitable threat- its potential to enhance detection and strengthen prevention measures is significant, but its success will always depend on the people who design, guide, and oversee its use. This balance between technological capability and human judgement is, in my view, the decisive factor in determining whether AI ultimately strengthens or undermines the integrity of AML efforts.

Final Closing Statement

The future of the fight against money laundering will nor rest solely on the sophistication of tools, but on the collective capacity-across institutions, regulators, and international bodies-to balance innovation, within a framework of fairness, transparency, and accountability. Only by aligning these principles can AI serve as a force that strengthens, rather than undermines, the integrity of the global financial ecosystem. In the end its resilience will be defined not by its most advanced capabilities, but by its ability to protect the most vulnerable points in the chain, ensuring that no link is left exposed to those who seek to exploit it.

REFERENCES

A

Alessa (2023) Customer Risk Scoring AML Model. Available at: https://alessa.com/blog/customer-risk-scoring-aml-model (Accessed: 1 May 2025).

B

Barocas, S., Hardt, M. and Narayanan, A. (2019) *Fairness and Machine Learning: Limitations and Opportunities*. Available at: https://fairmlbook.org (Accessed: 6 May 2025).

Basel Committee on Banking Supervision (2017) *Sound management of risks related to money laundering and financing of terrorism*. [online] Bank for International Settlements. Available at: https://www.bis.org/bcbs/publ/d405.pdf [Accessed 12 Jun. 2025].

Basel Committee on Banking Supervision (2014) Sound management of risks related to money laundering and financing of terrorism. Bank for International Settlements. Available at: https://www.bis.org/publ/bcbs275.pdf (Accessed: 12 Jun 2025).

Braun, V. & Clarke, V. (2006) 'Using thematic analysis in psychology', Qualitative Research in Psychology, 3(2), pp. 77–101. Available at: https://www.researchgate.net/publication/235356393_Using_thematic_analysis_in_psychology (Accessed: 21 July 2025).

Brookings Institution (2023). The U.S. and EU diverge on AI regulation: a transatlantic comparison and steps to alignment. Available at: https://www.brookings.edu/articles/the-eu-and-us-diverge-on-ai-regulation (Accessed: 6 July 2025).

Buchalter (2022) OCC Highlights Banks' Compliance Staffing Issues Even As Regulators Place More Compliance Demands on Banks and Place Executives at More Risk. [online] Buchalter. Available at: https://www.buchalter.com/publication/occ-highlights-banks-compliance-staffing-issues-even-as-regulators-place-more-compliance-demands-on-banks-and-place-executives-at-more-risk/ [Accessed 19 Jul. 2025].

C

D

Deloitte (2022) Explainable AI in banking: Enhancing model transparency and regulatory compliance, Deloitte Insights. Available at: https://www.deloitte.com/us/en/insights/industry/financial-services/explainable-ai-in-banking.html (Accessed: 1 Jun 2025).

Digital Banking Report (2024). State of AI in Retail Banking. [online] Digital Banking Report. Available at: https://www.opentext.com/media/report/state-of-ai-in-banking-digital-banking-report-en.pdf [Accessed 09 Jul. 2025].

E

European Banking Authority (2021) *Report on the use of machine learning for internal ratings-based models*. Follow-up report published 4 August 2023. Available at: https://www.eba.europa.eu/publications-and-media/press-releases/eba-publishes-follow-report-use-machine-learning-internal (Accessed: 1 Jun 2025)

European Commission (2021) Proposal for a Regulation on a European approach for Artificial Intelligence. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 (Accessed: 6 Jun 2025).

European Commission (2019) Ethics Guidelines for Trustworthy AI. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 (Accessed: 6 May 2025).

European Commission (2021) Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed: 6 May 2025).

European Union, 2015. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. Official Journal of the European Union, L141, pp.73–117. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L0849 [Accessed 23 Jun. 2025].

European Union, 2018. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849. Official Journal of the European Union, L156, pp.43–74. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843 [Accessed 23 Jun. 2025].

Europol (2021) Internet Organised Crime Threat Assessment (IOCTA) 2021. The Hague: European Union Agency for Law Enforcement Cooperation. Available at: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021?utm_source=chatgpt.com (Accessed: 19 Jun 2025).

EY (2021) *How AI is transforming financial crime compliance*. Available at: https://www.ey.com/en_us/insights/financial-services/how-ai-will-affect-compliance-organizations (Accessed: 1 Jun 2025)

F

Financial Action Task Force (FATF) (2023) Frequently asked questions: What is money laundering? Available at: https://www.fatf-gafi.org/en/pages/frequently-asked-questions.html#tabs-36503a8663-item-6ff811783c-tab (Accessed: 17 July 2025).

Financial Action Task Force (FATF), (2021). *Opportunities and Challenges of New Technologies for AML/CFT*. Paris: Financial Action Task Force. Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.inline.pdf [Accessed 26 Jun 2025].

Financial Action Task Force (FATF) (n.d.) *Frequently Asked Questions: How is money laundered?* [online] Available at: https://www.fatf-gafi.org/en/pages/frequently-asked-questions.html#tabs-36503a8663-item-6ff811783c-tab [Accessed 09 Jun. 2025].

Financial Action Task Force (FATF), (2013). Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals. Paris: FATF/OECD. Available at: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Mltf-vulnerabilities-legal-professionals.html [Accessed 12 Jun. 2025].

FATF, INTERPOL & UNODC (2025) *2025 Call to Action: Scaling up the global response to money laundering, terrorist financing and other forms of organised crime*. [online] FATF. Available at: https://www.fatf-gafi.org/en/publications/Fatfgeneral/FATF-INTERPOL-UNODC-2025-Call-to-Action.html [Accessed 10 Jun. 2025].

Flagright, 2024. *AML compliance in the era of artificial intelligence*. [online] Flagright. Available at: https://www.flagright.com/post/aml-compliance-in-the-era-of-artificial-intelligence [Accessed 29 Jun. 2025].

G

Global Financial Integrity (2017). *Illicit Financial Flows to and from Developing Countries: 2005–2014*. Washington, DC: (online) Available at: https://gfintegrity.org/report/illicit-financial-flows-to-and-from-developing-countries-2005-2014/ [Accessed 19 Jun. 2025].

H

Hilpisch, Y. (2020) Artificial Intelligence in Finance. Sebastopol, CA: O'Reilly Media.

I

International Labour Organization (2024). *Profits and poverty: The economics of forced labour.* [online] International Labour Organization. Available at: https://www.ilo.org/resource/news/annual-profits-forced-labour-amount-us-236-billion-ilo-report-finds [Accessed 5 Jun. 2025].

International Monetary Fund (IMF) (n.d.). Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT). [online] Available at: https://www.imf.org/en/Topics/Financial-Integrity/amlcft [Accessed 19 Jun. 2025].

International Monetary Fund (2001) *Financial System Abuse, Financial Crime and Money Laundering—Background Paper*. Washington, DC. (online) at: https://www.imf.org/external/np/ml/2001/eng/021201.pdf [Accessed: 3 July 2025].

J

K

Kallio, H., Pietilä, A.-M., Johnson, M. & Kangasniemi, M. (2016) 'Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide', Journal of Advanced Nursing, 72(12), pp. 2954–2965. Available at: https://doi.org/10.1111/jan.13031 [Accessed: 30 July 2025].

KPMG, (2023). Machine learning for anti-money laundering. [online] KPMG Belgium. Available at: https://kpmg.com/be/en/home/insights/2023/08/lh-machine-learning-for-anti-money-laundering.html [Accessed 19 Jun 2025].

Kranzberg, M. (1986). *Technology and History: "Kranzberg's Laws". Technology and Culture*, 27(3), pp. 544–560. [Accessed 03 August 2025].

L

Leslie, D. (2019). Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. The Alan Turing Institute. https://doi.org/10.5281/zenodo.3240529 (Accessed: 2 Jun 2025).

Lee, K-F. (2018) *AI Superpowers: China, Silicon Valley, and the New World Order*. Boston: Houghton Mifflin Harcourt. Available at: https://aisuperpowers.com/ (Accessed: 15 July 2025).

Levi, M. & Reuter, P. (2006) 'Money Laundering', *Crime and Justice*. Available at: https://orca.cardiff.ac.uk/id/eprint/3154/1/Levi%202006.pdf [Accessed 25 Jun. 2025].

Levi Michael (2012). How Well Do Anti-Money Laundering Controls Work in Developing Countries?', *Insights from Financial and Regulatory Crime Research*. Available at: https://scholar.google.com/scholar?q=How+Well+Do+Anti-Money+Laundering+Controls+Work+in+Developing+Countries+Levi [Accessed: 29 Jun 2025].

Lucinity (2025) 'Tackling alert fatigue in AML compliance with AI-powered case management', Lucinity Insights, 27 January. Available at: https://lucinity.com/blog/tackling-alert-fatigue-in-aml-compliance-with-ai-powered-case-management (Accessed: 1 Jun 2025).

M

Madinger, J. (2012) Money Laundering: A Guide for Criminal Investigators. BOCA RATON: CRC PRESS. Available at: https://research.ebsco.com/linkprocessor/plink?id=de22acde-d18a-3d1c-9878-f9a7b96d5f07 (Accessed: 29 April 2025).

Maple, C., Szpruch, L., Epiphaniou, G., Staykova, K., Singh, S., Penwarden, W., Wen, Y., Wang, Z., Hariharan, J. and Avramovic, P., 2023. The AI revolution: Opportunities and challenges for the finance sector. [preprint] arXiv. Available at: https://arxiv.org/abs/2308.16538 [Accessed 19 Jun. 2025].

Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021) 'A survey on bias and fairness in machine learning', *ACM Computing Surveys*, Available at: https://arxiv.org/pdf/1908.09635 (Accessed: 1 Jun 2025).

N

Nasdaq Verafin. (2024). *Global Financial Crime Report*. [online] Verafin. Available at: https://verafin.com/nasdaq-verafin-global-financial-crime-report/ [Accessed 5 Jun. 2025].

O

OECD, 2024. *Tax Crime Analytics Toolkit: Advanced Data Techniques for Enforcement*. [online] OECD. Available at: https://www.oecd.org/tax/crime/tax-crime-analytics-toolkit.htm [Accessed 20 Jul. 2025].

OECD, 2021. Advanced Analytics for Risk-Based Supervision. [online] Available at: https://www.oecd.org/finance/advanced-analytics-for-risk-based-supervision.htm [Accessed 20 Jul. 2025].

P

Q

R

Raji, I.D., Smart, A., White, R. et al. (2020). *Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing. arXiv.* Available at: https://arxiv.org/abs/2001.00973 (Accessed: 1 Jun 2025).

Ripjar, 2024. Case study: AI-integrated negative news screening in a Tier 1 APAC bank. [online] Ripjar. Available at: https://ripjar.com/blog/hkma-case-study-ai-integrated-negative-news-screening-in-a-tier-1-apac-bank/ [Accessed 02 Jul. 2025].

S

Sharman, J.C., 2011. *The Money Laundry: Regulating Criminal Finance in the Global Economy*. Ithaca, NY: Cornell University Press. Available at: https://www.cornellpress.cornell.edu/book/9780801450181/the-money-laundry/ [Accessed 15 July. 2025].

SWIFT (n.d.) Know Your Customer (KYC). Available at: https://www.swift.com/risk-and-compliance/know-your-customer-kyc (Accessed: 1 April 2025).

T

Taofeek, A. (2025) Ethical Considerations in Using Artificial Intelligence for AML Surveillance. Ladoke Akintola University of Technology. Available at: https://www.researchgate.net/publication/391662819_Ethical_Considerations_in_Using_Artificial_Intelligence_for_AML_Surveillance (Accessed: 6 July 2025).

Teradata, 2020. Danske Bank Saves Millions Fighting Fraud with Deep Learning and AI. [online] Teradata Case Study. Available at:

https://assets.teradata.com/resourceCenter/downloads/CaseStudies/CaseStudy_EB9821_Danske_Bank_Saves_Millions_Fighting_Fraud_With_Deep_Learning_and_AI.pdf [Accessed 19 Jul. 2025]

U

Unger, B. and van der Linde, D. (2013) *Research Handbook on Money Laundering*. Cheltenham: Edward Elgar Publishing.

United Nations Office on Drugs and Crime (UNODC), (n.d.) *Money-laundering*. [online] Available at: https://www.unodc.org/unodc/en/money-laundering/overview.html [Accessed 5 Jun. 2025].

United Nations Office on Drugs and Crime (UNODC), (2023) *Illicit Financial Flows: Trafficking in persons and migrant smuggling*. [online] Available at: https://www.unodc.org/documents/human-trafficking/2023/New_publications/GLOACT_Study_on_Illicit_Financial_Flows_-_Final.pdf [Accessed 10 Jun. 2025]

U.S. Department of the Treasury (n.d.) *Money laundering*. [online] Available at: https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance/money-laundering [Accessed 10 Jun. 2025].

Unites States Senate (2012). U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History. Washington, DC: United States Senate Permanent Subcommittee on Investigations. (online) Available at: https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/PSI%20REPORT-HSBC%20CASE%20HISTORY%20(9.6)2.pdf [Accessed: 29 Jun 2025].

V

W

World Bank (2022). *Financial Market Integrity. [online] World Bank.* Available at: https://www.worldbank.org/en/topic/financialmarketintegrity [Accessed 09 Jun. 2025].

World Bank (2011). The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It. Washington, DC: (online) Available at: https://star.worldbank.org/sites/star/files/puppetmastersv1.pdf [Accessed 29 Jun. 2025].

World Bank (2018) *Are global banks cutting off customers in developing and emerging economies?* [online] Available at: https://www.worldbank.org/en/news/feature/2018/05/02/are-global-banks-cutting-off-customers-in-developing-and-emerging-economies [Accessed 19 Jul. 2025].

World Bank (2022) Preventing Money Laundering and Terrorist Financing, World Bank Group. Available at: https://documents1.worldbank.org/curated/en/099532507212213583/pdf/IDU04f85b34a0f6dc04f19083f307136897d2cb6.pdf (Accessed: 1 Jun 2025).

World Bank Group, International Finance Corporation (IFC) (2018) *How a Know-Your-Customer Utility Could Increase Access to Financial Services in Emerging Markets (EMCompass Note 59)*. Available at: https://documents1.worldbank.org/curated/en/133091547846776274/pdf/133879-EMCompass-Note-59-KYC-Utility.pdf (Accessed: 1 April 2025).

World Economic Forum (2020) *The AI Governance Journey: Development and Opportunities*. Available at: https://www.weforum.org/whitepapers/the-ai-governance-journey-development-and-opportunities (Accessed: 16 July 2025).

World Economic Forum. (2018). *The new physics of financial services: How artificial intelligence is transforming the financial ecosystem*. Cologny/Geneva: World Economic Forum. Available at: https://www3.weforum.org/docs/WEF_New_Physics_of_Financial_Services.pdf (Accessed: 01 July 2025).

World Economic Forum (2019). Navigating Uncharted Waters: A Roadmap to Responsible Innovation with AI in Financial Services. Available at: https://www.weforum.org/whitepapers/navigating-uncharted-waters (Accessed: 6 May 2025).

World Economic Forum (2019) *A framework for responsible limits on facial recognition: Use case: Flow management*. Available at: https://www.weforum.org/whitepapers/a-framework-for-responsible-limits-on-facial-recognition-use-case-flow-management (Accessed: 6 August 2025).

Wolfsberg Group (2022) Wolfsberg Guidance on Digital Customer Lifecycle Management. Available at: https://db.wolfsberg-group.org/assets/497de382-1b84-4b6a-aed2-5e627d7c81c9/Wolfsberg%20Guidance%20on%20Digital%20Customer%20Lifecycle%20Management%20(2022).pdf (Accessed: 1 May 2025).

X

Y

Z

Zafar, K., Majeed, A., Ullah, A., Shafait, F., & Mian, A. (2023). A Comprehensive Survey of Explainable Artificial Intelligence: Taxonomy, Challenges, and Future Directions. arXiv. https://arxiv.org/abs/2305.02012 (Accessed: 19 May 2025).

APPENDICES

Appendix A - Participants Information Sheet

Interviewee ID	Position	Industry Sector	Region	Type of Institutions	Age	Year of Experience
Interviewee 1	Compliance Senior	Bank	Central America	National	44	15
Interviewee 2	Compliance Junior	Audit	Asia	International	33	6
Interviewee 3	Treasury back office	Bank	North America	International	46	18
Interviewee 4	Portafolio Exchange	Bank	Central America	International	69	37
Interviewee 5	Compliance Senior	Bank	Europe	International	39	15
Interviewee 6	Compliance Senior	Bank	Central America	International	47	10
Interviewee 7	Portafolio Exchange	Bank	North America	International	53	24

Appendix B – Consent Form Spanish

Estimado/aparticipante:

Gracias por considerar participar en esta investigación. Esta entrevista forma parte de una tesis de maestría que tiene como objetivo comprender los desafíos actuales que enfrentan las instituciones financieras en el ámbito de la prevención del lavado de dinero (AML), así como explorar en qué medida la inteligencia artificial (IA) puede actuar tanto como facilitadora como potencial amenaza en el fortalecimiento de estos marcos.

Su participación es de gran valor para este estudio, ya que su experiencia profesional permitirá enriquecer la comprensión práctica del fenómeno desde una perspectiva institucional y humana. La entrevista tendrá una duración aproximada de entre 45 y 60 minutos, y se llevará a cabo de forma virtual mediante una plataforma acordada previamente (por ejemplo, Zoom o Microsoft Teams). Las preguntas se centrarán en su conocimiento y percepción sobre el uso actual y futuro de tecnologías como la IA en los sistemas AML, así como en los retos operativos, éticos y regulatorios que esto implica.

Confidencialidad y ética

- Toda la información proporcionada será tratada con estricta confidencialidad. En ningún momento se hará referencia a su nombre, institución o cualquier dato que permita su identificación. En la tesis se utilizarán etiquetas genéricas como "Oficial de Cumplimiento" o "Profesional del sector bancario".
- Los audios y transcripciones se almacenarán de forma segura y serán eliminados al finalizar el proceso de evaluación académica, conforme a las políticas éticas de investigación del National College of Ireland.
- La participación es completamente voluntaria. Usted puede rechazar responder cualquier pregunta o retirarse de la entrevista en cualquier momento, sin que ello tenga ninguna consecuencia.
- No se derivará ningún beneficio económico por su participación, pero su aporte contribuirá significativamente al conocimiento académico sobre un tema de alto impacto global.

Consentimiento

Si está de acuerdo con participar en esta entrevista bajo los términos expuestos, le agradezco que lo confirme expresamente por correo electrónico respondiendo con la frase: "He leído y comprendido los términos del consentimiento informado, y acepto participar en la entrevista." Muchas gracias nuevamente por su colaboración.

Appendix C – Consent Form English

Dear Participant,

Thank you for considering taking part in this research. This interview is part of a master's thesis aimed at understanding the current challenges faced by financial institutions in the field of Anti-Money Laundering (AML) prevention, as well as exploring to what extent Artificial Intelligence (AI) can act both as an enabler and as a potential threat in strengthening these frameworks.

Your participation is highly valuable to this study, as your professional experience will help enrich the practical understanding of the phenomenon from both an institutional and human perspective. The interview will last approximately 45 to 60 minutes and will be conducted virtually via a pre-agreed platform (e.g., Zoom or Microsoft Teams). The questions will focus on your knowledge and perception of the current and future use of technologies such as AI in AML systems, as well as the operational, ethical, and regulatory challenges involved.

Confidentiality and Ethics

- All information provided will be treated with strict confidentiality. At no point will your name, institution, or any data that could identify you be mentioned. Generic labels such as "Compliance Officer" or "Banking sector professional" will be used in the thesis.
- Audio recordings and transcripts will be securely stored and deleted upon completion of the academic evaluation process, in accordance with the research ethics policies of the National College of Ireland.
- Participation is entirely voluntary. You may choose not to answer any question or withdraw from the interview at any time, without any consequences.
- There will be no financial benefit from your participation, but your contribution will significantly enhance academic knowledge on a topic of high global relevance.

Consent

If you agree to participate in this interview under the stated terms, I kindly ask you to confirm explicitly by email by replying with the phrase:
"I have read and understood the terms of the informed consent, and I agree to participate in the interview."

Thank you once again for your collaboration.

Appendix D – Interview Spanish

Preguntas principales

1. ¿Cuáles son los desafíos operativos o estratégicos más urgentes que enfrentan hoy las instituciones financieras al implementar marcos AML?

2. ¿Cómo afecta la fragmentación regulatoria global la efectividad de los sistemas AML?

3. ¿Cómo equilibran las instituciones financieras la presión por innovar con IA y el cumplimiento ético/legal?

4. ¿Qué riesgos observas en una dependencia excesiva de la IA en estos sistemas?

5. ¿Qué mejoras concretas has observado en procesos AML a partir del uso de IA?

6. ¿La IA está logrando seguirle el paso a los esquemas complejos de lavado transnacional?

7. ¿Cómo afectan los factores humanos internos la implementación de IA en AML?

8. ¿Qué posibles sesgos o desigualdades estructurales podrían surgir con el uso de IA en AML?

9. ¿Qué marcos regulatorios o éticos crees que hacen falta para usar la IA responsablemente?

10. ¿Cómo debería evolucionar la relación entre analistas humanos y herramientas de IA en AML?

Agradecimiento y cierre

Agradezco sinceramente su tiempo y disposición para participar en esta entrevista. Su experiencia y perspectiva son fundamentales para enriquecer esta investigación, que busca aportar una mirada crítica y humana sobre el rol de la inteligencia artificial en los sistemas de prevención del lavado de dinero (AML).

Le reitero que toda la información que comparta será tratada con estricta confidencialidad. En ningún momento se revelará su identidad ni se vincularán sus respuestas con datos personales o institucionales. Su participación es completamente voluntaria y será utilizada exclusivamente con fines académicos.

Appendix E – Interview English

Main Questions

1. What are the most urgent operational or strategic challenges that financial institutions face today when implementing AML frameworks?
2. How does global regulatory fragmentation affect the effectiveness of AML systems?
3. How do financial institutions balance the pressure to innovate with AI and ethical/legal compliance?
4. What risks do you observe in an excessive reliance on AI in these systems?
5. What specific improvements have you observed in AML processes as a result of using AI?
6. Is AI managing to keep pace with complex transnational money laundering schemes?
7. How do internal human factors affect the implementation of AI in AML?
8. What possible biases or structural inequalities could arise from the use of AI in AML?
9. What regulatory or ethical frameworks do you think are needed to ensure the responsible use of AI?
10. How should the relationship between human analysts and AI tools in AML evolve?

Acknowledgement and Closing

I sincerely appreciate your time and willingness to participate in this interview. Your experience and perspective are essential to enriching this research, which seeks to provide a critical and human perspective on the role of Artificial Intelligence in Anti-Money Laundering (AML) systems.

I reiterate that all the information you share will be treated with strict confidentiality. At no point will your identity be revealed, nor will your responses be linked to any personal or institutional data. Your participation is entirely voluntary and will be used exclusively for academic purposes.