

The value of artificial intelligence deployment for anti-money laundering and counter-terrorism financing





The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at gsma.com

Follow the GSMA on Twitter/X: [@GSMA](https://twitter.com/GSMA)

Authors

Kennedy Kipkemboi, Director Public Policy and Advocacy Mobile Money, GSMA

Winnie Wambugu, Mobile Money Regulatory Specialist, GSMA

Co-authors

Stealth Africa LLP- Antony Ngige and Peris Wambui

Published January 2024

© 2024 - GSMA.

GSMA Mobile Money

The GSMA Mobile Money programme works to accelerate the development of the mobile money ecosystem for the underserved.

For more information, please contact us:

www.gsma.com/mobilemoney

mobilemoney@gsma.com

[@GSMAMobileMoney](https://twitter.com/GSMAMobileMoney)

Contents

1	Abbreviations	4
2	Introduction	5
2.1	Background on money laundering and terrorism financing	6
2.2	Overview of DFS and evolution of criminal activities	7
2.3	Aims and objectives of the report	7
2.4	Research methodology/approach	7
3	AI deployment and adoption in AML and CFT	8
3.1	Key highlights	9
3.2	Demystifying AI	11
3.3	Overview of AI adoption in AML/CFT and regulatory environment	11
3.3.1	Automated transaction monitoring in AML and CFT	13
3.3.2	KYC	13
3.3.3	Reduction of false positives and negatives	13
3.3.4	Behavioural analysis for risk assessment and customer due diligence	14
3.3.5	NLP for regulatory compliance and enhanced due diligence	14
3.3.6	AI technologies used for AML and CFT compliance	14
3.4	AI adoption and confidence in its use in AML and CFT in mobile money	15
3.4.1	Case study of AI deployment in AML for mobile money in Africa	17
3.5	Challenges of AI applications	18
3.6	Barriers to wider adoption of AI for AML and CFT	18
3.7	Challenges and limitations in AI deployment for money laundering and terrorism financing detection	19
3.8	Compliance challenges in the adoption of AI in AML and CFT	20
3.8.1	Critical measures to ensure safe adoption of AI in AML and CFT	21
3.8.2	Complexity of AI application to AML compliance tasks	22
3.8.3	Preparedness to address the challenges associated with AI	22
3.8.4	Engagement on AI-related compliance requirements	22
3.8.5	A standardised framework or guidelines for AI adoption	22
3.9	Policy and regulatory considerations	23
3.9.1	Measures for safe adoption of AI	24
4	Conclusions and recommendations	25
5	References	26

1

Abbreviations

Abbreviation	Description
AI	Artificial intelligence
AML	Anti-money laundering
CDD	Customer due diligence
CFT	Counter-terrorism financing
DFS	Digital financial services
FATF	Financial action task force
GDP	Gross domestic product
KYC	Know your customer
ML	Machine learning
NLP	Natural language processing
OECD	Organisation for Economic Co-operation and Development
PEP	Politically exposed person
RegTech	Regulatory technology
SAR	Suspicious activity report
STR	Suspicious transaction report

2

Introduction



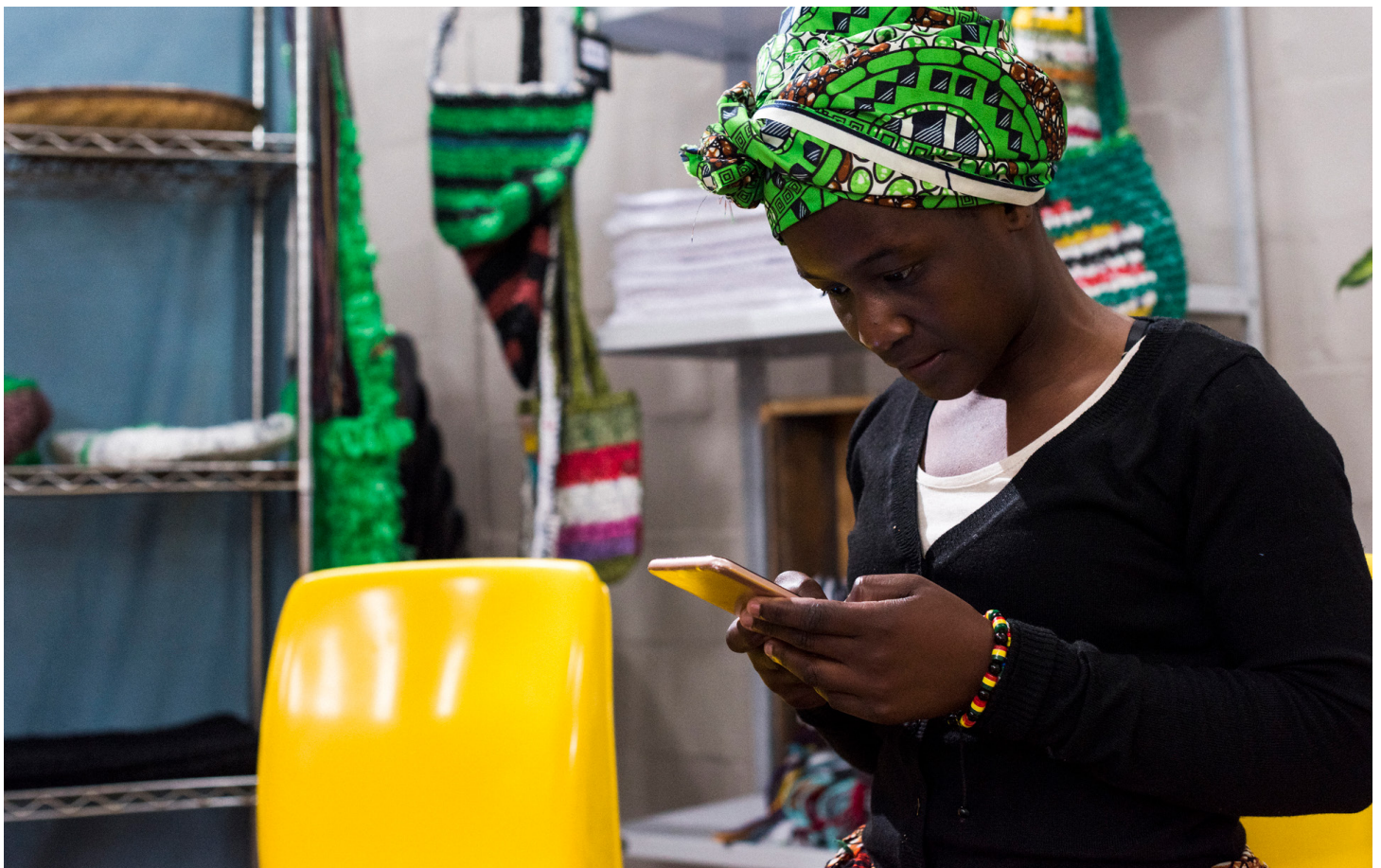
2.1 Background on money laundering and terrorism financing

The International Monetary Fund (IMF) defines money laundering as the process by which proceeds from criminal activity are disguised to conceal their illicit origin. Terrorism financing involves the solicitation, collection, or provision of funds with the intention of using them to support terrorist acts or organisations. Measures aimed at countering the financing of terrorism (CFT) seek to stop the flow of illegal cash to terrorist organisations. CFT is closely tied to anti-money laundering (AML) which refers to a set of laws, regulations, and procedures designed to prevent criminals from disguising illegally obtained funds as legitimate income. The IMF estimates the aggregated size of worldwide money laundering at approximately \$3.2 trillion, or 3% of global GDP.¹

Combating money laundering and terrorism financing is an enormous task that poses many risks, including but not limited to regulatory, reputational, and financial crime risks. The vulnerabilities that lead to AML/CFT risk factors can, however, be detected and monitored using artificial intelligence (AI). The GSMA is therefore creating a knowledge tool that can act as a point of reference for industry stakeholders and regulators in adopting AI to combat money laundering and terrorism financing.

\$3.2 tn  **OR** **3% of global GDP** 

Aggregate size of worldwide money laundering as estimated by the IMF



2.2 Overview of DFS and evolution of criminal activities

The financial industry is at risk on a global scale of regulatory and reputational implications due to money laundering and terrorism financing. Neglecting to address these activities can lead to severe penalties, erosion of customer confidence, and damage to the credibility of financial establishments.² The rapid evolution of digital financial services (DFS) has created opportunities for criminals to engage in complex transactions, and these transactions are often conducted in real time involving multiple layers – making it challenging to monitor and detect them using traditional AML and CFT methods. This calls for exploration of innovative solutions such as those based on AI.

2.3 Aims and objectives of the report

This report aims to provide an understanding of the current state of knowledge, practices and trends in the adoption of AI in AML/CFT. The report covers various AI techniques, their benefits, challenges, and the impacts they have on improving efforts to combat money laundering and terrorism financing. The report focuses on the following specific aspects:

- i. Examination of the deployment and adoption of AI by financial institutions and DFS providers in combating money laundering and terrorism financing
- ii. Assessment of the role of AI in critical compliance tasks in combating money laundering and terrorism financing and what is required for the industry to adopt AI
- iii. Assessment of safe adoption of AI by DFS that does not discriminate or result in a more pronounced digital divide for the unbanked and underserved
- iv. Illustration of the benefits of AI applications commensurate with their complexity and mitigation strategies for the potential compliance challenges they may bring
- v. Provision of policy and regulatory recommendations for sustainable AI solutions for the mobile money industry

2.4 Research methodology/ approach

This report is based on research on best practices related to the adoption of AI technologies in combating money laundering and terrorism financing. The report presents an examination of existing literature, academic papers, industry reports, case studies, expert interviews on AI deployment for AML and CFT and survey results in 16 countries in Africa, Asia and South America that have adopted AI in AML and CFT. The survey participants included 18 from mobile money service providers, three from other financial institutions and three from consultants in the mobile money and financial services industry.

The rapid evolution of digital financial services has created opportunities for criminals to engage in complex transactions.

¹Jorisch, Avi (2009) Tainted Money: Are We Losing the War on Money Laundering and Terrorism Financing? Red Cell Intelligence Group.

² IMF (2023). The Fight Against Money Laundering and Terrorism Financing

3

AI deployment and adoption in AML and CFT






This section gives an overview of AML and CFT practices, the regulatory environment, and the current state of adoption of AI in the mobile money and financial services markets.

We also discuss the effectiveness of AI adoption backed by case studies which show successful implementation.

Figure 1: Survey and literature review results.

3.1 KEY HIGHLIGHTS

Key AML/CFT challenges that can be addressed using AI

-  Automated transaction monitoring
-  Behavioural analysis for risk assessment and enhanced customer due diligence
-  Reduction of false positives and negatives



\$3.2 tn

OR 3% OF GLOBAL GDP

Aggregate size of worldwide money laundering as estimated by the IMF.

96%



Cited high cost and effort as AI adoption challenges

Number of organisations that cited the high cost and effort required for AI implementation as the major challenges hindering adoption.

87%



Find AI effective in AML/CFT

Number of organisations that have implemented AI and ML technologies for AML and CFT and find them to be effective, with more leaning towards 'very effective'.



96%

Recognise AI's impactful advantages

Positive perception of the benefits of AI in AML and CFT. The overwhelming majority of respondents acknowledge substantial benefits, which could translate into improved detection and prevention of financial crimes by AI.

54.2%



Report moderate to significant AI deployment in AML/CFT

Number of organisations surveyed reporting moderate to significant deployment of AI in efforts to combat money laundering and terrorism financing.

100%



Believe AI reduces false positives/negatives

Number of participants that believe AI can be useful in the reduction of false positives and negatives.

3.2 Demystifying AI

AI is the theory and development of computer systems able to perform tasks that normally require human intelligence. Examples include tasks such as visual perception, speech recognition, decision-making under uncertainty, learning, and translation between languages.³ A Forbes article explains that AI came about from rapidly increasing volumes of data which led to intensified research into ways it can be processed, analysed, and acted upon. Machines being far better suited than humans to this work, the focus was on training machines to do this in as 'smart' a way as possible.⁴

AI has the potential to handle several essential compliance tasks while addressing the key issues in current AML and CFT systems. Some examples highlighted in this study include automated transaction monitoring, reduction of false positives and negatives, behavioural analysis for risk assessment and customer due diligence, and natural language processing for regulatory compliance.

AI can be broadly categorised into several subsets, each focusing on different aspects or approaches to creating intelligent systems. AI subsets include:

Machine learning (ML): This involves algorithms that allow software to improve its performance on a task as it gains experience. It includes methods like supervised learning, unsupervised learning, and reinforcement learning. The term 'algorithm' refers to a set of rules or instructions designed to perform a specific task or solve a particular problem. Algorithms are used for data processing, calculation, automated reasoning, and other tasks. ML can be challenging with insufficient historical data to develop predictive insights.⁵

Deep learning (DL): DL is a subset of ML. DL uses neural networks with many layers (hence 'deep') to analyse various factors in large amounts of data. It's particularly effective for tasks like image and speech recognition.

Natural language processing (NLP): This area focuses on enabling machines to understand and interpret human language, allowing them to perform tasks like translation, sentiment analysis, and text generation.

Robotic process automation (RPA): This is AI technology that uses software robots or 'bots' to automate repetitive, rule-based tasks within business processes. RPA focuses on automating routine and mundane tasks that are typically performed by humans.

3.3 Overview of AI adoption in AML/CFT and regulatory environment

The Financial Action Task Force (FATF) recognises the need for innovative approaches to make AML and CFT measures faster, cheaper, and more effective.⁶ A subsequent report suggests actions for government authorities to advance the responsible development and use of new technologies for AML/CFT

which include creating an enabling environment for responsible innovation to enhance AML/CFT effectiveness, ensuring privacy and data protection, developing and communicating policies and regulatory approaches to innovation that are flexible, technology-neutral, outcomes-based and in line with the risk-based approach.⁷

³ Deloitte. (2018). Artificial intelligence: The next frontier for growth. Deloitte India.

⁴ Marr, B. (2017) The Complete Beginners' Guide to Artificial Intelligence. Forbes

⁵ Doppalapudi, P. K., Kumar, P., Murphy, A., Rougeaux, C., Stearns, R., Werner, S., & Zhang, S. (2022, October). The fight against money laundering: Machine learning is a game changer. McKinsey & Company

⁶ FATF, OECD. (2021) Opportunities and Challenges of New Technologies For AML/CFT.

⁷ FATF. (2021) Suggested Actions to Support the Use Of New Technologies For AML/CFT

⁸ Jullum, M., Løland, A., Huseby, R.B., Ånonsen, G., & Lorentzen, J. (2020). Detecting money laundering transactions with machine learning. Journal of Money Laundering Control, 23(1), 173-186.

Studies have identified three primary concerns associated with the current AML and CFT systems.⁸ These are maintaining up-to-date and relevant rules, having simplistic rule-based systems, and reducing false alerts. Respondents to the GSMA AI survey indicated that AML/CFT compliance tasks can use AI technologies in varying confidence levels as indicated below.

AI is widely regarded as highly applicable to most tasks related to AML/CFT, particularly those involving due diligence, monitoring, and screening activities. The confidence level in AI's applicability decreases as tasks become more related to internal processes which may involve more nuanced human judgment and less structured data.

These tasks are further explained below:

Figure 2: AML and CFT compliance tasks and confidence levels

AML/CFT Compliance Task	Confidence Level
Customer due diligence (CDD): AI can assist in automating identity verification and risk assessment, making the CDD process more efficient and accurate.	91.30%
Transaction monitoring: AI can analyze vast amounts of transaction data in real-time to identify suspicious patterns and anomalies, improving the detection of potential ML/FT activities.	95.65%
Suspicious activity reporting: AI can aid in flagging and prioritizing potentially suspicious activities, helping compliance teams to investigate and report them more effectively.	95.65%
Sanctions screening: AI can automate the screening of customers and transactions against sanctions lists and enhance the accuracy of matches.	95.65%
PEP (politically exposed person) screening: AI can streamline the identification and ongoing monitoring of PEPs by continuously monitoring news and political changes.	95.65%
Enhanced due diligence (EDD): AI can assist in identifying high-risk customers who may require enhanced due diligence and monitoring.	100%
Risk assessment and profiling: AI can enhance risk assessment models by incorporating various data sources and predicting customer risk profiles more accurately.	82.61%
Red flags identification: AI can help in the identification of red flags and suspicious indicators within transactions and customer activities.	78.26%
Technology and data management: AI can be used for data analysis, data quality control, and data management to ensure that compliance-related data is accurate and up to date.	39.13%
Compliance audits and testing: AI can aid in the automation of compliance audits and testing processes, making them more efficient and comprehensive.	30.43%
Employee code of conduct: AI can assist in monitoring and identifying potential violations of the employee code of conduct by analyzing communication and behavioral patterns.	26.09%

- AI is widely regarded as highly applicable to most tasks related to AML and CFT, particularly those involving due diligence, monitoring, and screening activities.
- The confidence level in AI's applicability decreases as tasks become more related to internal processes which may involve more nuanced human judgment and less structured data.

3.3.1 Automated transaction monitoring in AML and CFT

Transaction monitoring is the practice of discovering and reporting unusual transactions that could suggest money laundering, terrorism financing or other illegal activity. While traditional detection methods may struggle to keep pace with sophisticated criminal techniques, AI can analyse vast financial data to identify potential money laundering and terrorism financing activities through ML methods⁹. These technologies can analyse large volumes of financial data in real time, flagging suspicious transactions and patterns that may indicate money laundering and terrorism financing¹⁰. By automating the monitoring and diagnosing of money laundering and terrorism financing schemes, these systems can report suspicious activities, allowing financial institutions to take timely action to prevent money laundering and terrorism financing from occurring.¹¹

3.3.2 KYC

'Know your customer' (KYC) is the process of validating a customer's identification and background, as well as determining their risk profile and sources of cash. Biometrics, such as facial recognition, fingerprint scanning, or voice authentication, can be used by regulatory technology (RegTech) platforms to improve the accuracy and security of KYC processes. They can also employ ML and NLP to extract important information and insights about clients from unstructured data, such as social media posts, news articles, or public records. The effort required to address unintended bias in datasets includes using more diverse training datasets, improving algorithmic transparency, and regularly testing AI systems for fairness across different demographic groups.

3.3.3 Reduction of false positives and negatives

A false positive is a result which wrongly indicates that a particular condition or attribute is present – for example, a result indicating that a mobile money transaction is suspicious when it is not. A false negative on the other hand is a result which wrongly indicates that a particular condition or attribute is absent – for example, a result indicating that a mobile money transaction is not a suspicious activity when it is.

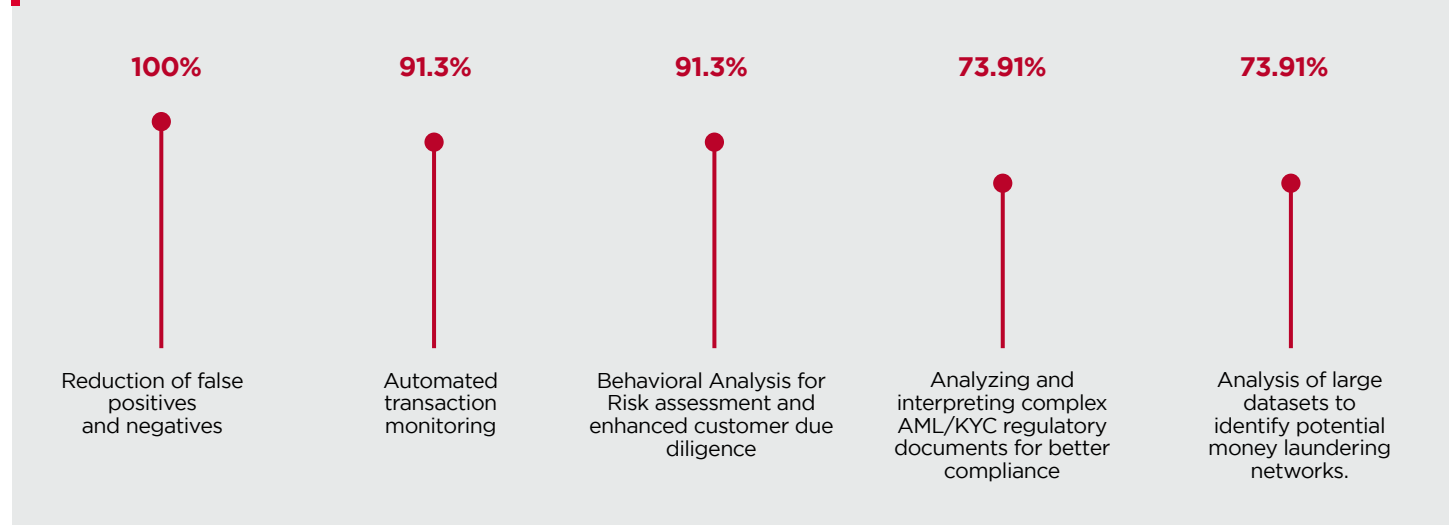
Standard rule-based systems are configured to detect specific actions and then fire off an alert. These rules sometimes pick out legitimate transactions. This would be a challenge as the volume of transactions increases

and AML analysts find themselves spending a lot of time investigating false positives.

Reducing false positives and negatives is a crucial aspect of AML and CFT efforts, and the use of AI can significantly contribute to achieving this goal. One way to reduce these errors is the AI feedback loop (also known as closed-loop learning), which is the process of leveraging the output of an AI system and corresponding end-user actions. All respondents (100%) in the GSMA AI Adoption for AML/CFT KYC survey indicated that AI could help reduce false positives as shown below:

Figure 3:

AML/CFT challenges that can be addressed using AI



⁹ Pavlidis, G. (2023). Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era. *Journal of Money Laundering Control*, 26(7), 155-166. <https://doi.org/10.1108/jmlc-03-2023-0050>

¹⁰ Utami, R., & Septivani, A. (2022). The Role of Automated Monitoring Systems in Detecting Money Laundering Activities. *Journal of Financial Crime*, 19(1), 123-140.

¹¹ Ibid

AI is seen as highly effective in reducing false positives and negatives, which is a common issue in AML and CFT, where accurate identification of suspicious activities is crucial. There is also high confidence in AI's role in automated transaction monitoring (91.30%) and behavioural analysis (91.30%), which are key areas for identifying and preventing money laundering and terrorism financing activities.

3.3.4 Behavioural analysis for risk assessment and customer due diligence

Behavioural analysis allows financial institutions to detect unusual patterns and anomalies in transactions, enabling them to assess the risk associated with specific activities. Additionally, customer due diligence (CDD) measures, which involve evaluating and understanding customer behaviour, play a crucial role in combating money laundering and terrorism financing. By employing AI technologies, such as ML algorithms and DL approaches, institutions can enhance their capabilities in analysing vast amounts of data to identify suspicious activities and predict potential money laundering and terrorism financing behavior. AI in AML and CFT not only addresses the challenges faced by financial institutions in onboarding politically exposed persons (PEPs) but also contributes to curbing financial cybercrime, fraud, and cyberattacks, thereby having significant implications for the global economy and society.¹²

59% of participants in the GSMA AI for AML and CFT survey ranked suspicious activity detection as the most complex AML task to automate using AI.

The survey results are illustrated below. Suspicious activity detection is perceived as the most complex AI application in the context of AML and CFT compliance. This could be due to the nuances of identifying illicit activities that are deliberately concealed within normal transaction patterns. This perception could guide where organisations might focus their efforts in terms of resource allocation, training, and development of AI capabilities.

3.3.5 NLP for regulatory compliance and enhanced due diligence

NLP models can be used to analyse and interpret regulatory documents. This technology ensures better adherence to complex AML/CFT regulations and reduced compliance costs. Mobile money services can leverage NLP in AI to ensure compliance with stringent AML/CFT regulations while streamlining the compliance process. NLP can be used to analyse and interpret large volumes of financial data, identify patterns, and detect suspicious activities that may indicate money laundering or terrorism financing. By using AI-powered NLP algorithms, mobile money service providers can automate the monitoring and analysis of transactions, enabling them to identify potential risks and take appropriate actions promptly and accurately.¹³

NLP can add value in many ways including automated monitoring of regulatory changes, risk assessment in CDD, screening and background checks, identification of beneficial ownership, and enhanced analysis of suspicious activity reports (SARs).



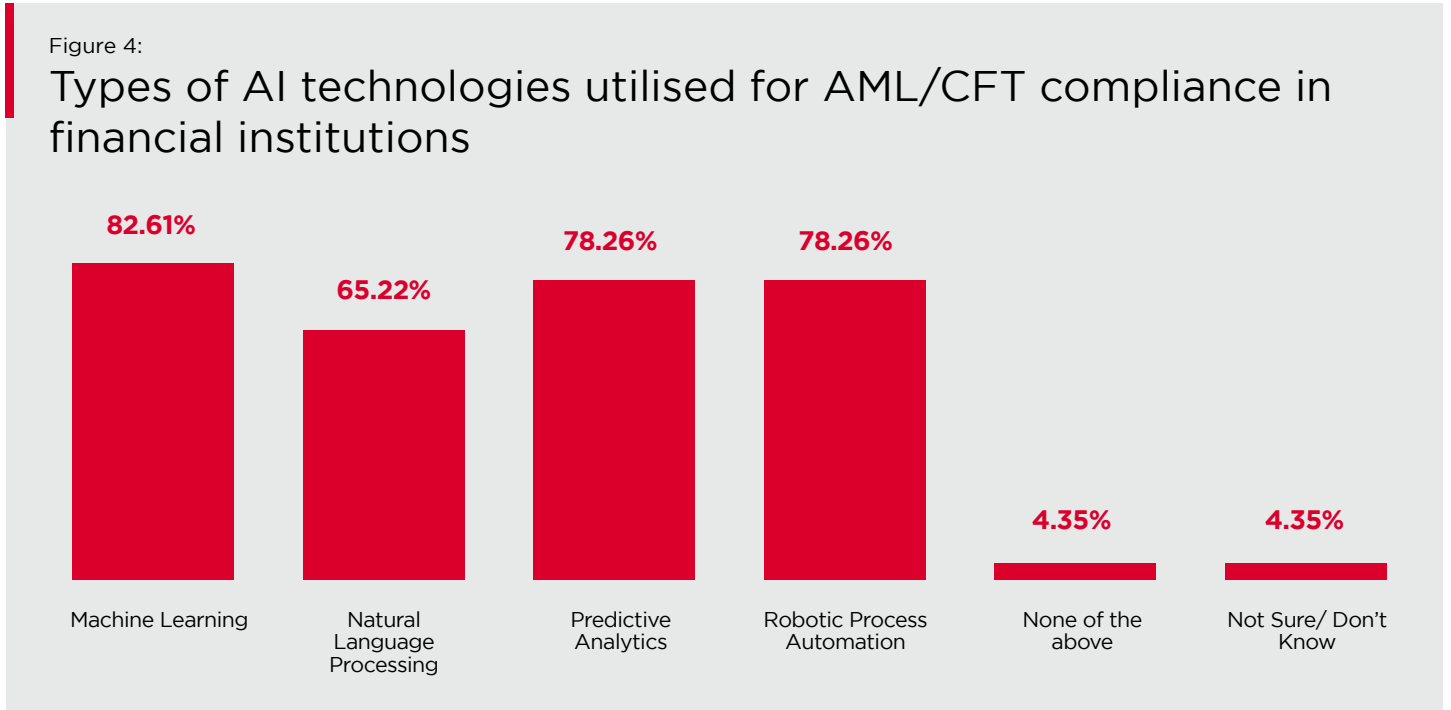
¹² Nicholls, J., Kuppa, A., & Le-Khac, N. (2021). Financial cybercrime: a comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. Ieee Access, 9.

¹³ Pavlidis, G. (2023). Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era. Journal of Money Laundering Control, 26(7).

3.3.6 AI technologies in use for AML and CFT compliance

Overall, AI technologies are an integral part of the compliance strategies for institutions in combating money laundering and terrorism financing, with varying degrees of adoption for different technologies.

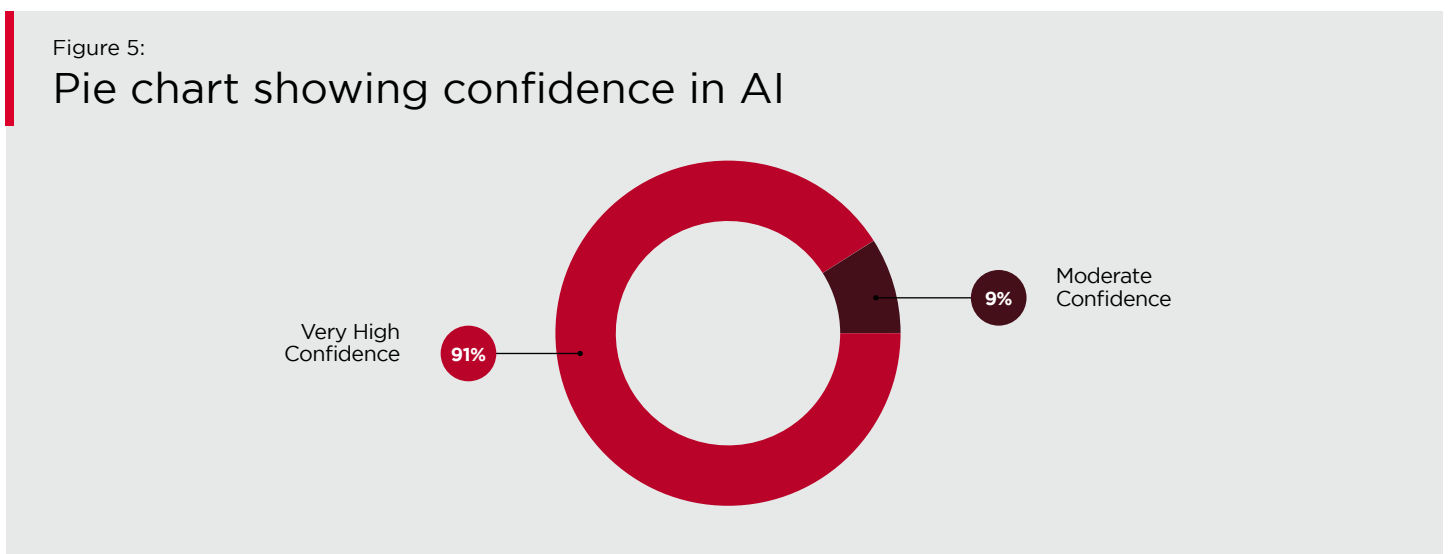
ML is the leading AI technology employed by institutions for AML/CFT compliance, reflecting its pivotal role in identifying patterns and anomalies that could indicate fraudulent activities, with 82.61% of our survey respondents indicating it as the top form of AI technology in use as shown below:



Predictive analytics and RPA are also commonly used (both at 78.26%), which supports their roles in forecasting potential risks and streamlining compliance processes respectively.

3.4 AI adoption and confidence in its use in AML and CFT in mobile money

AI is also being deployed to enhance AML and CFT efforts in mobile money. Survey respondents indicated high levels of confidence in AI in AML and CFT compliance as shown below:



In addition, 86.95% of the organizations that have implemented AI and ML technologies for AML and CFT find them to be effective, with more leaning towards 'very effective' as shown below:

Figure 6:

Effectiveness of deployed Artificial Intelligence and Machine Learning in AML and CFT in respondent organizations

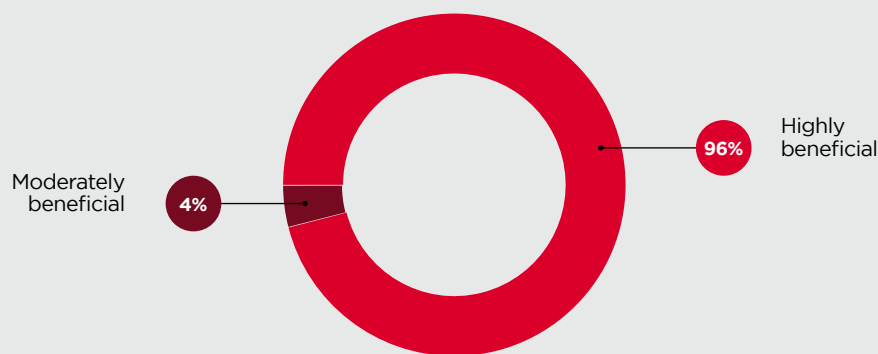


34.78% of responding organisations regard these technologies as moderately effective, which could indicate that they are in the early stages of implementation or that they face challenges in fully leveraging the technologies.

A very small percentage have not implemented AI and ML at all for AML and CFT, which may suggest a gap in adoption that could be due to various reasons such as lack of resources, expertise, or organisational readiness.

Figure 7:

Pie chart showing expected benefits of each AI application



Further, 96% of respondents as shown above acknowledge substantial benefits of AI. This includes improved detection and prevention of financial crimes. The comparatively small number of respondents viewing the benefits as moderate may indicate that there are still some challenges to be addressed or that AI applications have not yet been fully leveraged within their organisations. The disproportionate preference towards the 'highly beneficial' option underscores the potential value that financial institutions place on AI in enhancing their compliance processes and the importance of continuing to develop and integrate AI solutions in this field.

3.4.1 Case study of deployment of AI in AML for mobile money in Africa

This case study is based on key points from an interview with M-PESA Africa - a mobile money service provider with operations across Africa in 7 countries. M-PESA Africa has deployed AI technology in six countries which include Kenya. The deployment of AI in AML and CFT within the mobile money sector across several African countries presents a pioneering approach to financial security. The key learnings from the interviews include:



AI application in AML and CFT: AI is used effectively for customer profiling, watchlist screening, KYC alerts, batch processing, and monitoring suspicious activities and transactions. RPA is the primary AI technology employed, highlighting a focus on automating repetitive tasks. One of the most notable successes of AI in this sector is the reduction in Turnaround Time (TAT) for closing alerts from 30 to 5 minutes per case.



Regulatory landscape: Although regulators have largely allowed the use of AI in AML and CFT, one of the key considerations that needs to be addressed is the integration of data protection laws, bearing in mind that the use of cloud-based solutions may require cross-border transfer of data. AI systems used by this mobile money provider primarily use cloud storage, which is preferred for its cost-effectiveness and accessibility while ensuring robust security and data privacy.



Cost and implementation: The initial high cost of deploying AI technology, including licensing and implementation, is an industry barrier that cuts across all participants. There is high demand for AI services and as such organisations face integration and deployment delays. This is mostly due to the shortage of skilled AI professionals in the region. Compliance and risk monitoring professionals require training in AI to ensure effective and speedy deployment.



Data management: High-quality data is critical for AI because it serves as the foundation upon which AI systems learn, make decisions, and generate insights. The data therefore needs to be cleaned to remove errors, and categorised, formatted and labelled to properly guide the learning process.



Accuracy, transparency and reliability: Feedback loops are crucial in AI to reduce errors and enhance performance, allowing users to correct issues such as false positives and negatives in image recognition, thereby improving its reliability in its application in CDD).

By using rule-based systems in parallel with AI systems, organisations can benefit from the advanced capabilities of AI while maintaining a level of understanding in their decision-making processes.



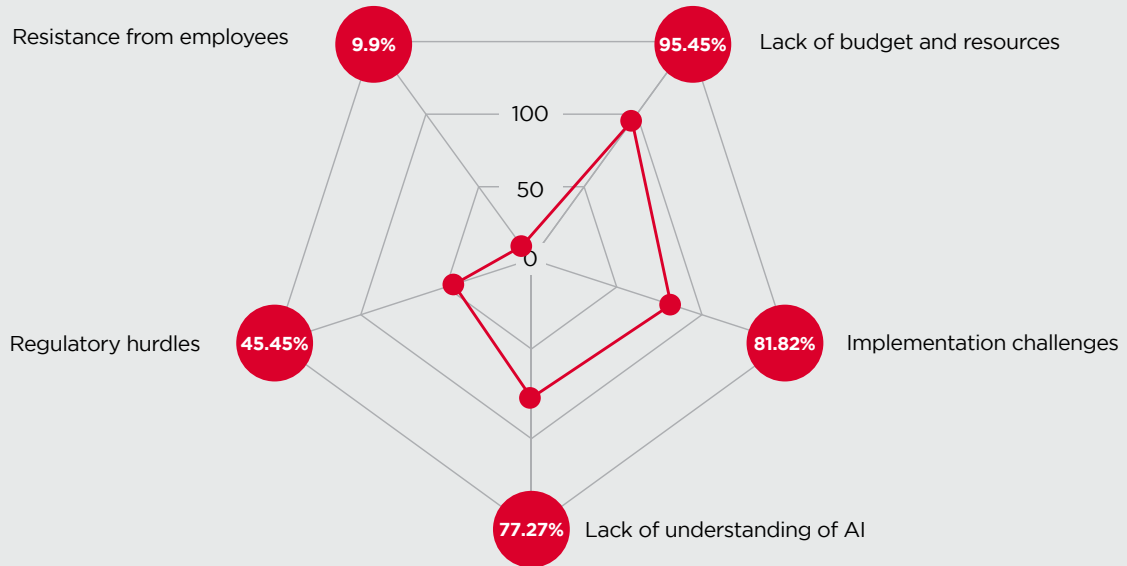
3.5 Challenges of AI applications

As shown in the case study above, AI has huge benefits but also challenges including lack of transparency, costs and implementation hurdles, data management and false positives issues that require attention. This is consistent with our survey results as shown below:

3.6 Barriers to wider adoption of AI for AML/CFT compliance

Figure 8:

Barriers to wider adoption of AI in AML/CFT compliance



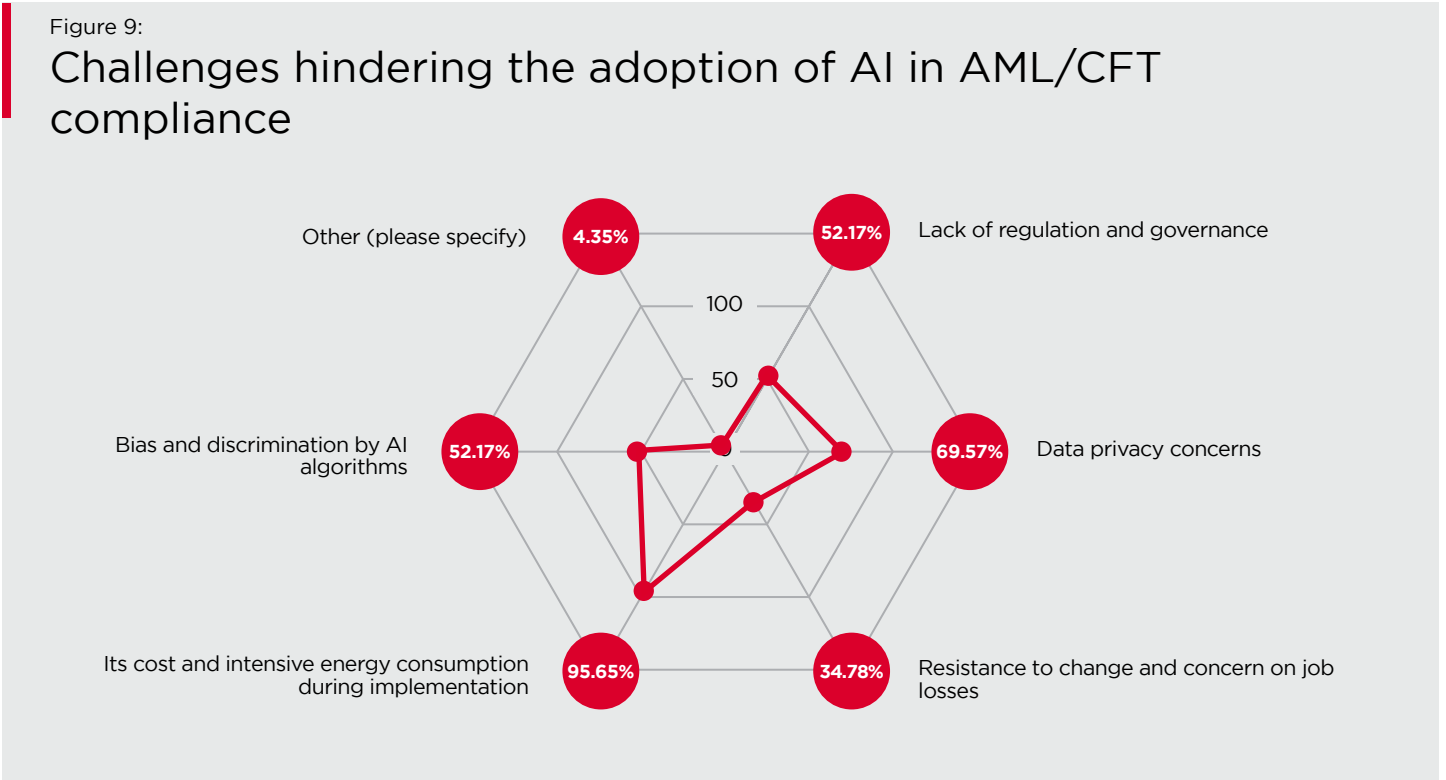
Financial constraints and implementation difficulties are the most significant barriers to adoption of AI for compliance purposes in the financial industry. While understanding AI and regulatory challenges are also concerns, they appear to be secondary to the more immediate issues of budget and practical implementation.

Employee resistance is considered the least significant barrier, which may suggest that the workforce is either adaptable to AI adoption or that the other challenges are so significant that employee resistance is overshadowed.



3.7 Challenges and limitations in AI deployment for money laundering and terrorism financing detection

The survey results indicate that 96% of survey participants ranked the high cost and effort required for AI implementation as the major challenges hindering adoption. The survey results for the challenges and limitations in AI deployment for money laundering and terrorism financing detection are as illustrated below:



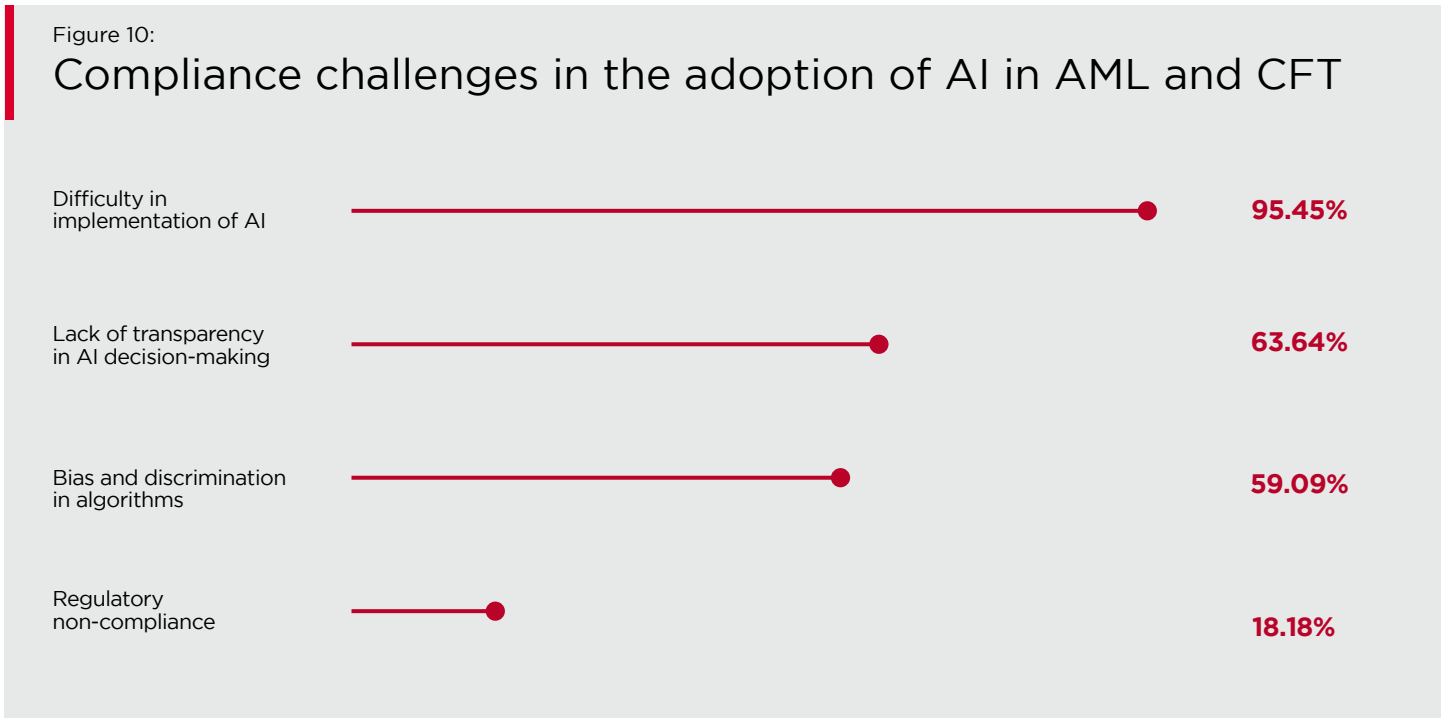
The financial investment and effort required to implement AI solutions is considered the most significant challenge to adoption in the context of AML and CFT compliance. Data privacy is also a major concern, reflecting the sensitive nature of financial data and the stringent regulations that protect such information.

The need for clearer regulation and governance frameworks for AI in financial services is acknowledged as a notable obstacle. Concerns about bias and discrimination in AI algorithms are recognised, which is particularly relevant in compliance settings where fairness and accuracy are paramount. Resistance to change and worries about job losses due to AI adoption are present but are not viewed as the primary challenges.



3.8 Compliance challenges in the adoption of AI in AML and CFT

In the survey, we asked respondent to state what the most prevalent compliance challenges in the adoption of AI in AML and CFT compliance are. The results show that 95% of the respondents find difficulty in implementation of AI to meet AML and CFT requirements as the top challenge. This highlights the need for focused efforts to overcome these barriers to facilitate the effective use of AI in the financial industry. The result of the survey is illustrated below:



Practical difficulties in implementing AI are seen as the most significant challenge to its adoption for AML and CFT compliance. This suggests a consensus among respondents that implementing AI in compliance processes is a significant hurdle, likely due to factors such as complexity, cost, and the need for specialised knowledge. Transparency and bias are also critical issues that need to be addressed to ensure trust and fairness in AI systems.

A substantial number of respondents could be worried about the 'black box' nature of some AI systems, where it is not clear how the AI arrived at a particular decision. There are concerns that AI systems may inadvertently perpetuate existing biases or create new forms of discrimination. Regulatory compliance, while less of a challenge compared to the others, remains an important consideration for organisations using AI in financial compliance.



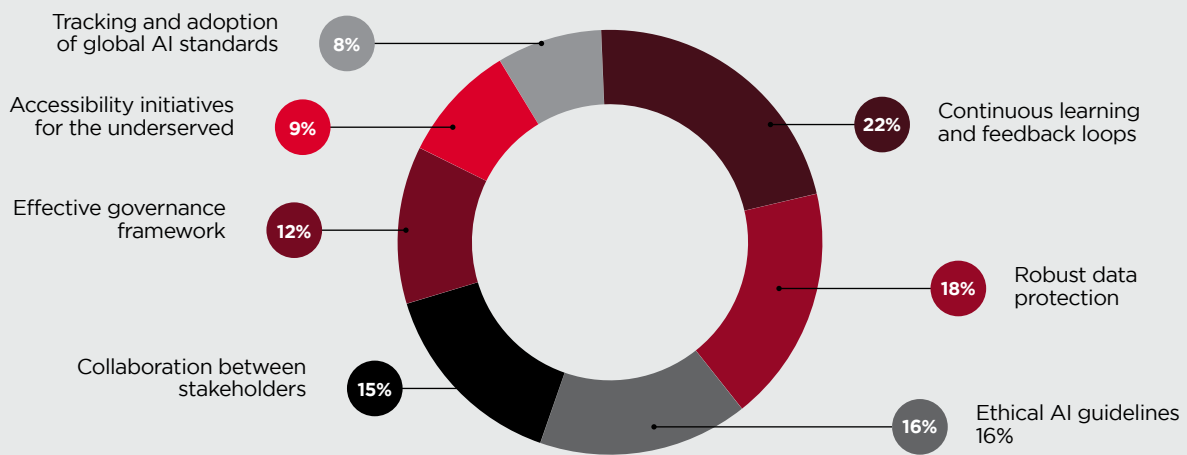
3.8.1 Critical measures to ensure the safe adoption of AI in AML and CFT

There is strong consensus on the need for continuous improvement and ethical considerations in AI systems used for AML and CFT. Data protection and collaborative efforts also rank highly, showing a multi-faceted approach is valued for the safe adoption of AI in this sector.

Lower importance attached to global standards may suggest that this aspect is still evolving, and organisations may be waiting for a more unified and comprehensive approach to emerge. The survey results are illustrated below:

Figure 11:

Pie chart showing critical measures to ensure the safe adoption of AI in AML and CFT

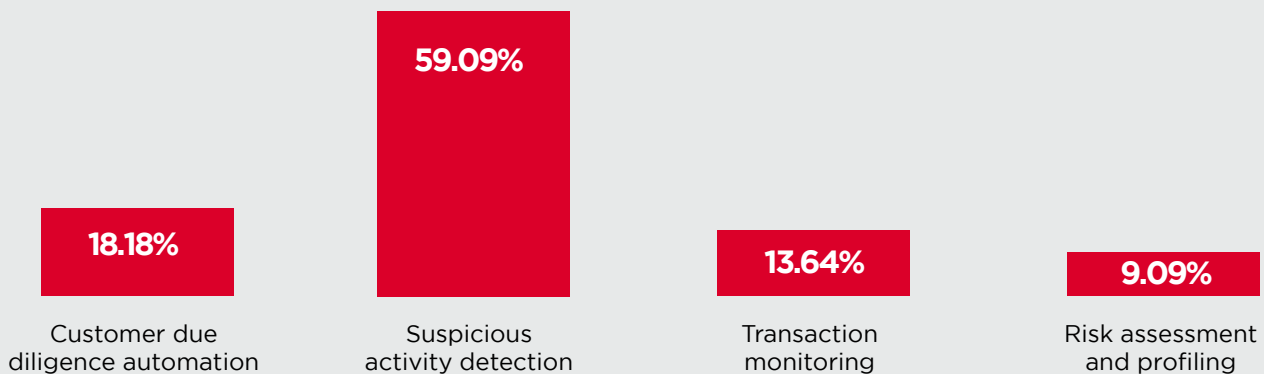


3.8.2 Complexity of AI application in AML compliance tasks

59% of participants ranked suspicious activity detection as the most complex AML task to automate using AI. This is likely due to the need for sophisticated analysis, high accuracy, and the consequences of false positives or negatives. Suspicious activity detection is perceived as the most complex AI application in the context of AML and CFT compliance. This could be due to the nuances of identifying illicit activities that are deliberately concealed within normal transaction patterns. The ranking also indicates that while other areas such as CDD automation, transaction monitoring, and risk assessment are complex, suspicious activity detection is seen by respondents as more challenging. This perception could guide where organisations might focus their efforts in terms of resource allocation, training, and development of AI capabilities. The survey results are illustrated below:

Figure 12:

AI applications in AML/CFT compliance based on their complexity and potential compliance challenges



3.8.3 Preparedness to address the challenges associated with AI

Only 25% of respondents felt that their organisations are fully prepared to address the challenges associated with AI such as bias, discrimination, and data privacy concerns.

The reported level of preparedness among organisations varies, with a small tendency towards only slight preparedness. However, a significant portion of organisations also felt moderately prepared or slightly prepared, indicating that many have taken some steps to address the ethical and privacy challenges AI presents. The fact that 75% of organisations considered themselves not fully prepared suggests there is still much work to be done in the field to ensure organisations are ready to handle the intricacies of AI implementation, particularly in sensitive areas like AML/CFT compliance. This report can serve as a call to action for organisations to evaluate their preparedness and potentially seek additional resources or strategies to improve their stance on AI deployment.

3.8.4 Engagement on AI-related compliance requirements

Only 16% of the organisations surveyed stated that they engage regularly with the regulatory bodies or other industry players to keep updated on AI-related compliance requirements. 41.7% of the organisations surveyed take a slightly laid-back approach to engagement on AI compliance issues. 42% of organisations either don't engage or rarely engage. This suggests there may be gaps in knowledge or awareness of AI compliance within the industry. This could be a point of concern given the rapidly evolving nature of AI technology and the corresponding need for up-to-date regulatory knowledge to ensure compliance and mitigate risks associated with AI deployment. This could also be because of the limited number AI deployments in DFS so far.

3.8.5 A standardised framework or guidelines for AI adoption

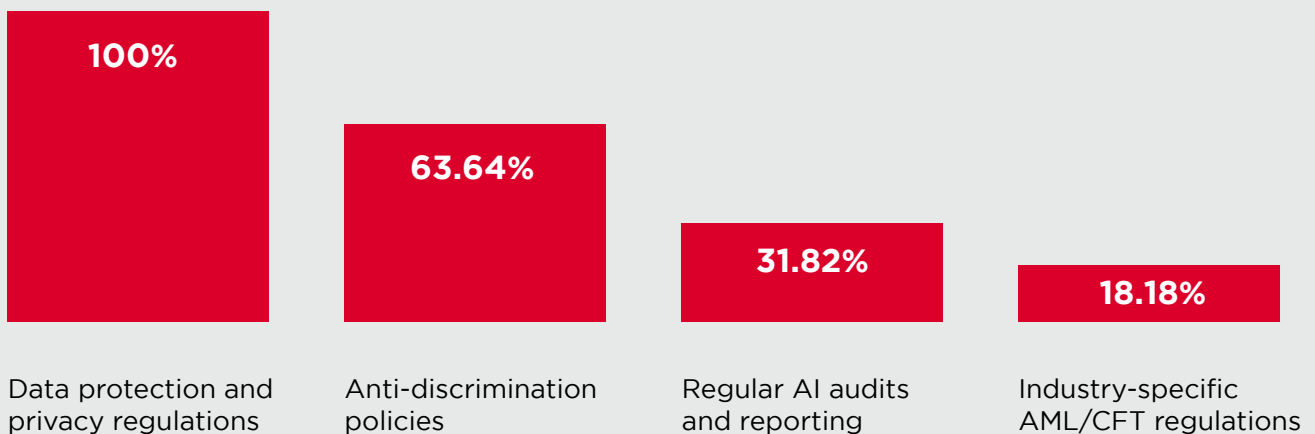
An overwhelming 96% participants believed there is need for a standardised framework or guidelines for AI adoption in the financial industry to combat money laundering and terrorism financing. This underscores the perceived urgency and importance of a framework or guidelines. This consensus also suggests that industry stakeholders are likely to support the development and implementation of such frameworks or guidelines.

3.9 Policy and regulatory considerations

Below is our summary of the results obtained based on the survey on whether there are key policies and regulatory considerations for sustainable AI solutions.

Figure 13:

Graph illustrating the survey results of the key policy and regulatory considerations for sustainable AI solutions for sustainable AI solutions in AML/CFT



There was a very strong consensus among respondents that data protection and privacy are crucial in the context of AI for AML and CFT. Anti-discrimination policies also play a significant role, indicating awareness of the social implications of AI. Regular audits and industry-specific regulations were considered important but not prioritised as highly, which may suggest that respondents see these as supplementary to the foundational concerns of data protection and the ethical use of AI. The percentages reflect the relative emphasis that financial institutions, DFS and other stakeholders place on these considerations in the context of AI for compliance.

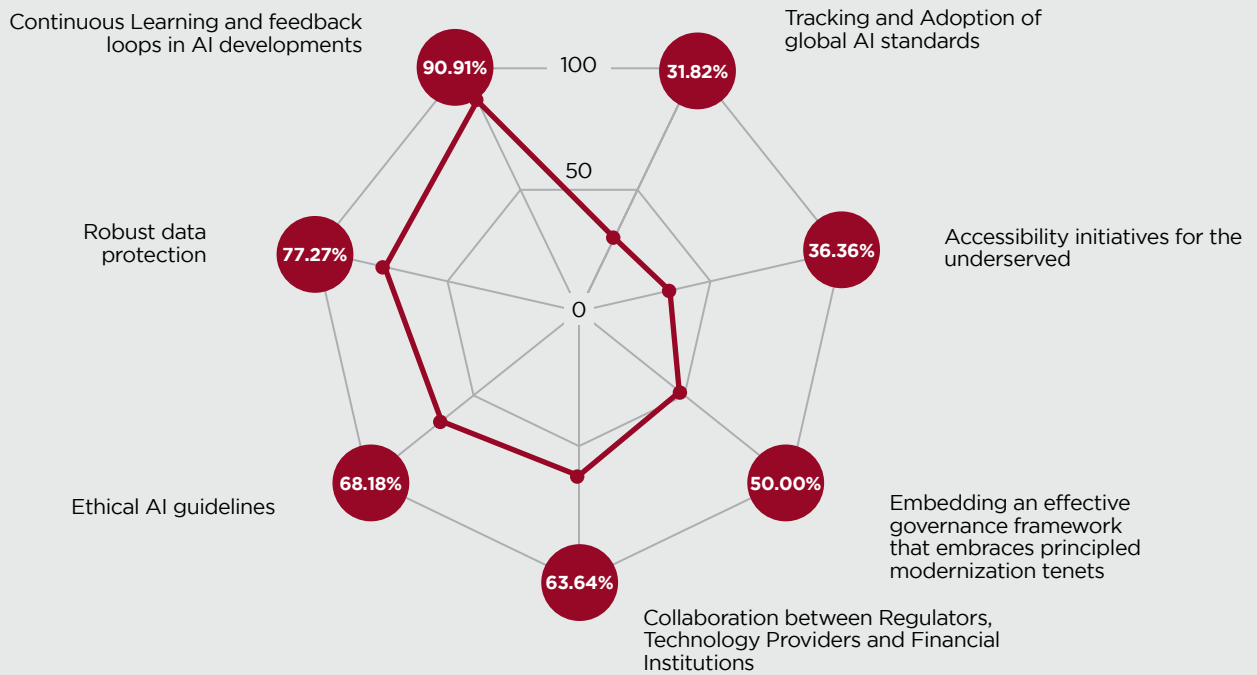
Anti-discrimination policies also play a significant role, indicating awareness of the social implications of AI

3.9.1 Measures for safe adoption of AI

90.91% of survey respondents indicated continuous learning and feedback loops as the most crucial measure for safe adoption of AI for AML and CFT. This could be because continuous learning and feedback loops empower AI systems to evolve, learn from new data, enhance accuracy, and adapt to emerging threats while minimising AI challenges such as bias and discrimination. Respondents also indicated that robust data protection, ethical AI guidelines and collaboration among stakeholders are crucial measures for safe adoption of AI as shown in the graph below:

Figure 14:

Measures that can be taken to ensure the safe adoption of AI in AML and CFT



The G7 recently released a draft of guiding principles for organisations interested in advanced AI systems, as part of their ongoing Hiroshima AI Process. These principles, which build upon the OECD’s own AI Principles, seek to promote safety, security, and trust in the development and use of advanced AI globally.¹⁴ They offer guidance for organisations working on various forms of AI, including foundational models and generative AI. Covering a range of important topics such as human rights, democracy, risk management, transparency, and accountability, these principles are meant to be a dynamic and adaptable document, reflecting ongoing developments in technology.

In addition, the G7 members have also committed to creating an international code of conduct for organisations involved in advanced AI development, based on the principles set forth in this draft.¹⁵

Other jurisdictions have instruments such as executive orders establishing new standards for AI safety and security, data privacy, consumer protection, and promoting innovation and competition.¹⁶

¹⁴ European Commission. (2021). International draft guiding principles for organizations developing advanced AI systems. <https://digital-strategy.ec.europa.eu/en/library/international-draft-guiding-principles-organizations-developing-advanced-ai-systems>

¹⁵ European Commission. (2021). International draft guiding principles for organizations developing advanced AI systems.

¹⁶ The White House. (2023, October 30). FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence.

4

Conclusions and recommendations



The difficulties posed by money laundering and terrorism financing have grown in complexity and scope in an era where the global financial system is becoming more connected and digital. This calls for radical transformation in our approach to combating these threats. Traditional methods, reliant on manual scrutiny and rule-based systems, are becoming obsolete in the face of sophisticated criminal strategies, particularly in the realm of DFS.

In this report, AI emerges not just as a technological option but a critical necessity for effective and advanced AML, CFT and KYC processes in mobile money. This requires collaborative efforts from all stakeholders to embrace AI's potential responsibly, balancing innovation with ethical practices, regulatory compliance, and financial inclusion. The report finds widespread recognition of AI's benefits and the need for concerted action to overcome the challenges associated with its adoption in the fight against money laundering and terrorism financing.

The integration of AI in AML and CFT within the mobile money sector demonstrates both the potential and challenges of this technology. A balanced approach that combines AI with human expertise and clear regulatory frameworks is essential for overcoming these challenges and maximising the benefits of AI in financial security.

The decision to implement AI in the fight against money laundering and terrorism financing involves weighing the costs against the benefits. While the initial and ongoing costs can be significant, the benefits of improved efficiency, enhanced detection capabilities, and regulatory compliance are substantial in the context of the growing sophistication of financial crimes - meaning the benefits of AI in enhancing the capabilities to combat money laundering and terrorism financing seem to outweigh the costs, especially when considering the long-term benefits.

To advance the field of AI for AML and CFT research and action, it is crucial to consider the digital transformation of AML and CFT in view of the various principles and acts.

Policy makers should consider tax incentives or grants for research into more efficient

Additionally, the deployment of AI for AML and asset recovery is considered the dawn of a new era, aligning with principles such as the FATF San Jose principles, the OECD principles for AI, and the proposed EU Artificial Intelligence Act.¹⁷

Policymakers can work on formulating clear guidelines and standards for AI in financial services, providing a legal and ethical framework. The creation of AI-specific regulations is crucial, as indicated by 95.83% of the survey respondents who either agreed or strongly agreed on the need for a standardised framework for AI adoption in the financial industry. These regulations should be dynamic and adaptable, providing clear guidelines for ethical AI use, and non-prescriptive.

Policymakers should consider tax incentives or grants for research into more efficient AI systems - clear legislative frameworks that balance data privacy with the benefits of AI could be developed and collaborate with technology providers and privacy advocates to ensure robust data protection measures are in place.

There is a clear need for the regulators to work with FATF, FATF regional counterparts, and other AML and CFT compliance bodies, in driving the use of AI for AML and CFT. This effort should include seeking technical assistance from development partners to support policymakers in implementing AI-driven guidelines. Additionally, regulators could also leverage regulatory sandboxes to test and refine AI-focused regulatory approaches in a controlled setting.

In conclusion, there is a need for collaboration between regulators, technology providers, and digital financial institutions to develop cohesive approaches to AI regulation in AML and CFT, as highlighted by 63.64% of survey respondents, which is consistent with the literature reviewed underscoring the importance of global cooperation on AI regulation. Further important measures according to this research include continuous learning and feedback loops in AI developments, robust data protection and ethical AI guidelines.

¹⁷ Pavlidis, G. (2023). Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era. *Journal of Money Laundering Control*, 26(7).

5

References



Jorisch, Avi (2009) Tainted Money: Are We Losing the War on Money Laundering and Terrorism Financing? Red Cell Intelligence Group.

IMF (2023). The Fight Against Money Laundering and Terrorism Financing.

Deloitte. (2018). Artificial intelligence: The next frontier for growth. Deloitte India.

Marr, B. (2017) The Complete Beginners' Guide to Artificial Intelligence. Forbes

Doppalapudi, P. K., Kumar, P., Murphy, A., Rougeaux, C., Stearns, R., Werner, S., & Zhang, S. (2022, October). The fight against money laundering: Machine learning is a game changer. McKinsey & Company

FATF, OECD, (2021) Opportunities and Challenges of New Technologies For AML/CFT.

FATF, (2021) Suggested Actions to Support the Use of New Technologies For AML/CFT

Jullum, M., Løland, A., Huseby, R.B., Ånonsen, G., & Lorentzen, J. (2020). Detecting money laundering transactions with machine learning. Journal of Money Laundering Control, 23(1), 173-186.

Pavlidis, G. (2023). Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era. Journal of Money Laundering Control, 26(7),

Utami, R., & Septivani, A. (2022). The Role of Automated Monitoring Systems in Detecting Money Laundering Activities. Journal of Financial Crime, 19(1), 123-140.

Nicholls, J., Kuppa, A., & Le-Khac, N. (2021). Financial cybercrime: a comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. IEEE Access, 9.

European Commission. (2021). International draft guiding principles for organizations developing advanced AI systems. <https://digital-strategy.ec.europa.eu/en/library/international-draft-guiding-principles-organizations-developing-advanced-ai-systems>

The White House. (2023, October 30). FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence.

GSMA Head Office

1 Angel Lane
London EC4R 3AB
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601

