



Journal of Financial
Supervisors Academy

Advancing Financial Regulation and Supervision

Publication Date: 2nd November 2026

Volume 02

ISSN: 3104-4948

e-ISSN: 3104-4956





Volume 02

Publication Date: 2nd November 2026

Advancing Financial Regulation and Supervision

This volume, titled “**Advancing Financial Regulation and Supervision**” focuses on the ongoing evolution of financial regulation and supervision as authorities respond to geopolitical developments, technological innovation, and the pursuit of more effective and proportionate oversight. The articles are organized to cover key themes such as cross-border supervision and geopolitical risk, the regulation of emerging technologies and payments, and the advancement of smarter, outcomes-based supervisory practice, reflecting the comprehensive approach needed to support well-functioning, resilient, and inclusive financial markets.



2.2
Professional Insight

How can AI Improve Risk-Based AML Supervision and Financial Inclusion

Marica Ciantar



Author's Bio



Av. Marica Ciantar is a Public Prosecutor within the Office of the Attorney General in Malta specialising in financial crime and computer misuse prosecutions. After obtaining her warrant to practice law in 2023, she pursued a Master of Science in Blockchain and Distributed Ledger Technologies at the University of Malta.

Av. Ciantar continues to contribute to research in criminal law and technology, both independently and through her work with the Office of the Attorney General. Her academic interests include cybercrime and the intersection of emerging technologies with criminal justice.

Cover Proposal and Confirmations

This article examines whether artificial intelligence (AI) can be used to strengthen the Financial Action Task Force's (FATF) risk-based approach to anti-money laundering (AML) supervision whilst addressing the challenges of de-risking and financial exclusion. Whilst the risk-based approach intends to promote proportionality and effectiveness, its implementation has often resulted in defensive compliance practices which prioritise risk avoidance over risk management. This article argues that AI has the potential to improve risk differentiation, monitoring and supervisory confidence thus enabling a financial institution to manage higher-risk relationships more effectively rather than excluding them.

This article conceptualises the interaction between AI, the risk-based approach and financial inclusion as a governance and supervisory challenge rather than solely a technological issue. It demonstrates how AI may reduce de-risking by enabling better assessment of customer and transactional risk, which is consistent with FATF principles. Finally, it examines the pertinent technical and regulatory challenges associated with AI adoption in anti-money laundering to analyse how AI can support both supervisory effectiveness and financial inclusion.

This article is original, has not been published elsewhere and is not under consideration by another journal.

Abstract

The FATF's risk-based approach aims to promote proportionality yet, in practice, its implementation has frequently resulted in de-risking and financial exclusion. The aim behind this article is to examine whether AI can enhance risk-based anti-money laundering supervision while supporting financial inclusion. AI can improve risk differentiation, monitoring and supervisory confidence thus enabling a financial institution to manage higher-risk relationships more effectively rather than excluding them. Nevertheless, the benefits of AI are conditional on governance safeguards such as explainability, human oversight and regulatory clarity. This article demonstrates how, when aligned with FATF principles, AI can support both anti-money laundering effectiveness and financial inclusion as mutually reinforcing objectives.

Introduction

According to a 2025 Europol report, the United Nations Office on Drugs and Crime has estimated that between 2% and 5% of the global gross domestic product, which amounts to €715 billion and €1.87 trillion, is laundered annually worldwide. This scale of illicit activity underscores the continuing importance of the FATF framework and the necessity of robust anti-money laundering efforts by financial institutions.¹

The Financial Action Task Force (“FATF”) is an inter-governmental body mandated to set international standards and promote the effective implementation of legal, regulatory, and operational measures to safeguard the integrity of the international financial system. In furtherance of its mandate, the FATF has promulgated Forty Recommendations, which constitute the principal global framework for the prevention and suppression of money laundering, terrorist financing, and proliferation financing. These Recommendations require states to adopt frameworks and strategies for mitigating financial crime risks, whilst imposing preventative obligations upon financial institutions. Financial institutions shall comply with obligations such as: the undertaking of customer due diligence, the maintenance of adequate records, the submission of suspicious transaction reports, and the identification and verification of beneficial owners of legal persons. The Recommendations further emphasise the necessity of effective supervisory and enforcement mechanisms, including proportionate, dissuasive, and effective sanctions for non-compliance and emphasise the importance of international cooperation which help give full effect to the mission of the FATF.²

A foundational principle of the FATF framework is the risk-based approach, which underpins efforts to safeguard the integrity of the financial system. Whilst the risk-based approach operates on the idea that resources should be allocated according to priorities, ensuring that the most significant risks receive the most attention,³ financial institutions often err excessively on the side of caution when applying the risk-based approach, particularly given the practical challenges it presents. Unlike rule-based compliance, the risk-based approach requires institutions to exercise judgement and calibrate controls to varying levels of risk, a process that can be complex, resource-intensive, and costly. As a result, institutions often adopt overly restrictive policies or avoid customers perceived as higher risk, even where risks could be managed through proportionate mitigation measures. Such overly cautious practices contribute to financial exclusion, undermining access to financial services and conflicting with the FATF’s emphasis on proportionate, risk-sensitive measures,

“It is not the intention of the FATF to impose rigid standards or to mandate a single operating process that would negatively affect the payment system or financial inclusion.”⁴

1 Europol, ‘Criminal Finances and Money Laundering’ <<https://www.europol.europa.eu/crime-areas/criminal-finances-and-money-laundering>> accessed 31 January 2026.

2 Financial Action Task Force (FATF), ‘International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations’ <<https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>> accessed 24 January 2026.
Hereinafter referred to as ‘The FATF Recommendations’

3 FATF, ‘Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High-Level Principles and Procedures’ <<https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatfguidanceontherisk-basedapproachtocombatingmoneylaunde ringandterroristfinancing-highlevelprinciplesandprocedures.html>> accessed 24 January 2026.
Hereinafter referred to as ‘The FATF High Level Principles and Procedures’

4 The FATF Recommendations (n2)

New technologies and technological developments, including contemporary applications of artificial intelligence ('AI'), offer the potential to assist financial institutions in meeting their anti-money laundering obligations and complying with the FATF Recommendations, supporting financial inclusion objectives.

The need for AI based solutions stems from the vast amounts of data which financial institutions must process, which data may be both structured and unstructured and can be used to identify patterns and predict whether financial transactions may be associated with illicit activities.⁵ AI further enables financial institutions to carry out real-time monitoring of transactions, have more comprehensive and dynamic risk assessments and strengthen governance and oversight.⁶

In light of the above, this article examines how financial institutions can advance financial inclusion under a risk-based approach to anti-money laundering, while leveraging AI to enable the onboarding of higher-risk individuals in a controlled and proportionate manner.

01

The Risk Based Approach

Recommendation 1 on 'Assessing risks and applying a risk-based approach' of the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, The FATF Recommendations ('The FATF Recommendations') establishes the obligation of States to assess risks and apply a risk-based approach. FATF Recommendation 1 positions the risk-based approach as a foundational principle underpinning the broader anti-money laundering framework established by the FATF Recommendations.⁷

The risk-based approach operates at both national and institutional level. States are required to identify, assess and understand the risks affecting their financial system via National Risk Assessments and ensure that their anti-money laundering frameworks respond to the identified risks, whilst financial institutions must assess and manage the financial risks arising from their own business relationships and activities and take measures to mitigate such risks.

The principle behind the risk-based approach is that measures taken by States shall be proportionate to the risks identified with resources allocated according to the amount of risk presented. Hence, the resources allocated should be proportionate to the risk assessed and the application of the recommendations shall also follow this

5 M Brewczyńska, 'Combating Financial Crime with AI at the Crossroads of the Revised EU AML/CFT Regime and the AI Act' (2026) New Journal of European Criminal Law <<https://doi.org/10.1177/20322844251408680>> accessed 1 February 2026.
Hereinafter referred to as, 'M Brewczyńska 2026'

6 FATF, 'Opportunities and Challenges of New Technologies for AML/CFT' (July 2021) <<https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html>> accessed 27 January 2026.
Hereinafter referred to as, 'FATF New Technologies Report'

7 The FATF Recommendations (n2), Recommendation 1

risk-based approach.⁸ Proportionality requires that, where multiple measures are capable of effectively mitigating financial crime risks, the option that is least burdensome – while taking financial inclusion considerations into account – should generally be preferred. This may include, for example, the application of simplified measures in lower-risk scenarios, such as simplified due diligence.⁹

According to the FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures ('FATF Guidance on the Risk Based Approach (RBA)'),¹⁰

*"There are no universally accepted methodologies that prescribe the nature and extent of a risk-based approach. However, an effective risk-based approach does involve identifying and categorizing money laundering risks and establishing reasonable controls based on risks identified."*¹¹

Financial institutions adopt a combination of practices to ensure that their anti-money laundering regimes are in line with the risk posed and these typically include measures such as, customer due diligence, monitoring of transactions and record-keeping. The fundamental principle underpinning the risk-based approach is that compliance measures should not be implemented in a uniform manner across all individuals or entities but are systematically adjusted – either intensified or relaxed – based on the specific level of risk posed by each customer. This tailored application allows financial institutions to allocate resources more efficiently and effectively, ensuring enhanced oversight where higher risks are identified, such as with politically exposed persons or complex financial transactions, while allowing for simplified procedures in lower-risk scenarios.

In emphasising the importance of an appropriate and effective control structure for managing money laundering risks, the FATF Guidance on the RBA acknowledges both the value and the inherent limits of risk-based compliance. It recognises that a risk-based approach should be reasonably designed and effectively implemented, so that controls are proportionate to the risks identified and resources are allocated where they are most needed. At the same time, FATF accepts that even a well-calibrated risk-based framework does not eliminate the risks relating to financial crime altogether, describing it as not a "zero failure" approach.¹² Money laundering methods, typologies, and enabling technologies continue to evolve, meaning that regulated entities and supervisory authorities are unlikely to detect every illicit transaction or misuse of the financial system.

The FATF recognises that anti-money laundering measures should focus on reducing identifiable risks, not on eliminating all risk. Hence, financial institutions should maintain a high degree of flexibility and adapt their preventative, detective, and monitoring controls in response to evolving threats.¹³ In doing so, financial institutions

8 Ibid

9 FATF, 'Guidance: Financial Inclusion and Anti-Money Laundering and Terrorist Financing Measures' (June 2025) <<https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Financial-Inclusion%20-Anti-Money-Laundering-Terrorist-Financing-Measures.pdf.coredownload.pdf>> accessed 25 January 2026
Hereinafter referred to as 'FATF, Guidance on Financial Inclusion'

10 The FATF High Level Principles and Procedures (n3)

11 Ibid

12 FATF, 'Guidance for a Risk-Based Approach, The Banking Sector' (October 2014) < <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Banking-Sector.pdf.coredownload.pdf> > accessed 25 January 2026
Hereinafter referred to as 'FATF Guidance for The Banking Sector'

13 FATF, High Level Principles and Procedures (n3)

are expected to adopt more stringent measures when the risk is higher and less stringent measures when the risk is low. It is imperative that the risk-based approach is not to be interpreted as exempting financial institutions from mitigating risks when the risk is low but to apply measures such as simplified due diligence measures.¹⁴

02

The Risk-Based Approach and Financial Exclusion

The risk-based approach, as previously outlined, is not without its consequences as for financial institutions to implement this approach effectively, increased operational costs may be incurred, and improper adoption can result in substantial fines. At times, this leads financial institutions to adopt stricter rules for certain customers, leading to financial exclusion and de-risking of legitimate businesses and consumers.¹⁵ Whilst the FATF has tried to mitigate these risks, de-risking and financial exclusion remain a challenge.¹⁶

De-risking occurs when institutions terminate or restrict customer relationships to avoid perceived risk rather than manage it through proportionate controls. Although de-risking is inconsistent with the proper application of the risk-based approach, it remains strongly associated with it in practice, particularly where financial institutions adopt an overly cautious interpretation of anti-money laundering obligations. Financial institutions may engage in de-risking for a range of interconnected reasons, including profitability concerns, rising compliance and operational costs, fear of supervisory or enforcement action, reduced institutional risk appetite, and reputational considerations. In turn, such practices may result in unfair exclusion, as entire groups of customers—often including vulnerable or underserved individuals—can be denied access to financial services on the basis of broad assumptions and generalised risk indicators rather than an individualised and proportionate assessment of their actual risk.¹⁷

De-risking is a significant driver of financial exclusion, as it may result in customers being denied access to, or removed from, the formal financial system. Financial exclusion can arise from a range of socio-economic and structural factors, including limited access to financial services and concerns relating to trust, privacy, and the security of personal data.¹⁸ Moreover, as financial services increasingly transition online, individuals with limited digital literacy may face additional barriers to participation. This can be more pronounced among older persons, who may be less familiar with digital platforms and therefore more likely to rely on cash-based transactions rather than engaging with electronic payment systems.

It may be argued that de-risking, by excluding certain customers from the formal financial system, safeguards financial integrity by reducing exposure to money laundering risks. However, this reasoning is flawed, as it confuses

14 FATF Guidance for The Banking Sector (n12)

15 FATF, Guidance on Financial Inclusion (n9)

16 FATF, 'Mitigating the Unintended Consequences of the FATF Standards' (October 2021)
 <<https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Unintended-consequences-project.html>> accessed 24 January 2026
 Hereinafter referred to as 'FATF, Mitigating unintended consequences'

17 ibid

18 ibid

risk avoidance with risk management and undermines the proportionality that the risk-based approach is intended to achieve. Furthermore, financial exclusion should not be seen as an indicator of a lower money laundering risk. Rather, financial exclusion can push illicit financial activity outside the formal banking system, where transactions are less visible and therefore more difficult for authorities and financial institutions to detect and monitor.

Malta's National Risk Assessment of 2023 on Money Laundering, Terrorist and Proliferation Financing and Targeted Financial Sanctions¹⁹ has found that in August 2021, the 'high-risk' legal persons for concealment of beneficial owners for money laundering purposes were those that, inter alia, lacked a Maltese IBAN account and only an estimated 42% of all legal persons registered in Malta are deemed to be in possession thereof, resulting in the lack of visibility of financial activities.

The FATF has categorically held how de-risking does not comply with its Standards,

*"Financial exclusion not only harms individuals and businesses but can also represent a real risk to achieving effective implementation of FATF Standards by driving financial activity into unregulated channels."*²⁰

In discouraging financial exclusion and hence promoting financial inclusion, the FATF Recommendations recognise that, in limited circumstances, and where money laundering risks have been assessed as low, countries may decide not to apply certain Recommendations to specific categories of financial institutions. The FATF framework further clarifies that such exemptions should be confined to narrowly defined and justified situations, including instances where the relevant risks are demonstrably low or where a financial activity is conducted only on an occasional or limited basis.²¹ The flexibility provided by the Recommendations allows states to adjust their policies in the interest of financial inclusion.²²

03

Financial Inclusion, the FATF Recommendations and Anti-Money Laundering

Financial inclusion and anti-money laundering are not mutually exclusive, rather, they can be mutually reinforcing. Greater access to regulated financial services reduces the extent to which individuals and businesses are compelled to rely on cash-based transactions or unregulated payment channels. By encouraging participation in the formal financial system, financial inclusion increases the traceability of transactions and enhances transparency, thereby strengthening the capacity of both financial institutions and competent authorities to

19 National Coordinating Committee on Combating Money Laundering and Funding of Terrorism (December 2023), 'National Risk Assessment' <https://ncc.gov.mt/wp-content/uploads/2024/10/PublicNRA_Dec2023-1.pdf> accessed 1 February 2026

20 FATF, Guidance on Financial Inclusion (n9)

21 The FATF Recommendations (n2), Interpretive Note to Recommendation 1

22 FATF, Guidance for the Banking Sector (n12)

detect suspicious activity and mitigate the risk of financial crime.²³

Reliance on unregulated financial services may increase the vulnerability of legitimately unserved or underserved individuals and entities, exposing them to heightened risks of becoming victims of financial crime, unintentional facilitators, or even coerced participants. For example, individuals who resort to informal lenders, such as loan sharks, may face exploitative debt arrangements that can lead to serious forms of abuse, including coercion into criminal activity, forced labour, human trafficking, or acting as money mules to launder illicit funds.²⁴

Financial inclusion is recognised as an important driver of economic growth and sustainable development, including under the United Nations Sustainable Development Goals. It has also remained a priority for the G20 since the creation of the Global Partnership for Financial Inclusion and continues to feature prominently in the work of institutions such as the International Monetary Fund, the World Bank and the United Nations.²⁵

Financial inclusion refers to, *“both access to and active use of an adequate suite of regulated, appropriate, safe, convenient and affordable financial services by individuals (including households) and entities that would benefit from such services.”*²⁶ According to a FATF report published in June 2025 titled, ‘FATF Guidance, Financial Inclusion and Anti-Money Laundering and Terrorist Financing Measures’ (“the 2025 FATF Guidelines”), financial inclusion increased significantly between 2011 and 2021, with global account ownership rising by approximately 50%. Nevertheless, an estimated 1.4 billion adults worldwide still lack access to formal banking services or a mobile money account. Moreover, account ownership does not necessarily translate into meaningful usage, as in some cases new account holders continue to rely primarily on unregulated financial services for their day-to-day transactions.²⁷

Financial inclusion initiatives seek to address the needs of individuals and entities who lack access to regulated financial services (“unserved”) or whose access remains limited (“underserved”). For example, an individual may be considered underserved where; despite having formal access to financial services, they do not meaningfully use them due to factors such as cost, limited financial or digital literacy, lack of trust, or a perceived lack of utility. An individual may also be underserved should a financial institution go completely digital. The Malta Financial Services Authority’s (‘MFSA’) ‘Dear CEO’ letter highlighted this issue holding that certain demographics may be slower to adapt to digital services and cultural preferences for face-to-face interaction require financial institutions to embrace multiple channels when transitioning from traditional services to digital ones.²⁸

The concept of financial inclusion was initially understood primarily in terms of access to regulated financial services. However, it has since developed into a broader concept that also encompasses the effective and appropriate use of financial products and services, as well as the level of financial literacy needed to engage with

23 FATF, Guidance on Financial Inclusion (n9)

24 *ibid*

25 *ibid*

26 *ibid*

27 *ibid*

28 Malta Financial Services Authority, ‘Dear CEO Letter: Digitalisation Thematic Review’ (11 February 2025) < <https://www.mfsa.mt/wp-content/uploads/2025/02/Dear-CEO-Letter-Digitalisation-Thematic-Review.pdf> > accessed 1 February 2026
Hereinafter referred to as ‘MFSA, ‘Dear CEO’

them. Financial inclusion is therefore not solely concerned with access, but also with ensuring that individuals can meaningfully participate in the formal financial system through informed decision-making and an understanding of available financial products and services.²⁹

Financial inclusion may be promoted through the expansion of digital financial services. The FATF's 2025 guidance highlights that the digitalisation of payments, particularly government-to-person ('G2P') payments, can significantly enhance financial inclusion and strengthen payment integrity by requiring recipients to maintain a regulated account to receive electronic deposits. In this context, the FATF encourages digital financial inclusion and supports the use of non-face-to-face onboarding methods when these make sense according to the risk profile of the country and where these measures are proportionate to the risks associated with the relevant business relationship or activity. Nevertheless, digital financial services may not be accessible to all individuals, particularly considering persistent disparities in digital literacy and access. In response, governments have increasingly promoted financial literacy initiatives, which may improve consumer engagement with financial products and, in turn, support broader financial inclusion objectives.³⁰

04

Digital Financial Inclusion

In a March 2025 communication to the public, the MFSA found that 60% of clients are enrolled in mobile or internet banking thus, the use of digital services has increased nevertheless, although this shift is clear, a considerable number of persons still prefer face-to-face interactions, especially for complex financial matters; thus, a balance between digital innovation and traditional banking services must be maintained. Furthermore, in its 'Dear CEO' letter the MFSA has acknowledged how financial inclusion may be enhanced by digital means,

*"Data and digitalisation are rapidly transforming economies and communities, promoting inclusive growth, addressing inequities, and improving public service delivery, thus enabling the achievement of the Sustainable Development Goals (SDGs) which are part of the UN 2030 Agenda for Sustainable Development."*³¹

Digital financial inclusion may include business relations formed through non-face-to-face methods such as the onboarding of customers via the use of customer identification or verification measures relying on digital documents. To this end, the FATF Guidance on Digital Identity requires such identification and/or verification measures are done through *"reliable, independent digital ID systems, with appropriate risk mitigation measures in place, may pose a standard level of risk, or may even be lower risk"*, hence, it is necessary to adopt methods that provide an appropriate level of confidence that the system produces accurate and reliable results.

29 FATF, Guidance on Financial Inclusion (n9)

30 ibid

31 MFSA, 'Dear CEO' (n28)

Such digital ID systems could facilitate onboarding and customer due diligence measures and support ongoing due diligence and aid transaction monitoring.³²

In accordance with Recommendation 15 of the FATF Recommendations, countries and financial institutions shall assess the business environment of the day and identify and evaluate the developments in technology which affect the integrity of the financial system. Emerging technologies are not inherently beneficial or harmful but are frequently characterised as ‘dual-use’, hence, their impact depends on the manner in which they are deployed.

Financial services going digital and/or online helps modernise the industry, putting it up to par with the modern business environment of today, however, this does not come without its consequences. In fact, a rising trend in financial crime is using AI and deepfake technology to create accounts with financial institutions using deepfake technology to create pictures and documents of persons who do not exist (‘synthetic persons’) or else commit identity theft to open bank accounts in others’ names. To address these challenges, financial institutions may adopt measures such as cross-checking customer data against reliable sources and monitoring the behaviour of customers through behavioural profiling and location changes. The risk-based approach also allows financial institutions the flexibility to add post-transaction controls in case suspicious activity gets flagged.³³

The FATF’s 2025 guidance provides an illustrative example of how a Brazilian bank mitigates the risks associated with non-face-to-face services through a layered set of controls applied across the customer lifecycle. At the onboarding stage, the bank strengthens identity verification through facial biometrics, including liveness checks, and undertakes data and document validation by cross-referencing information against internal and external databases. These measures are complemented by Know Your Customer procedures designed to verify customer information, ensure consistency, and resolve any discrepancies. Risk mitigation is further supported through real-time transaction monitoring and post-transaction review mechanisms. Real-time monitoring may include enhanced user authentication measures, such as two-factor authorisation, behavioural profiling based on a customer’s digital habits and associated metadata, and customer communication to confirm anomalous activity. Artificial intelligence and machine-learning models are used to support the assessment of transaction risk by analysing variables such as transaction value, timing, and customer characteristics. Post-transaction monitoring may involve additional AI-enabled risk analysis, typology-specific controls, the identification of indicators associated with remote transactions, and the application of structured risk-classification tools to support ongoing customer profiling and risk management. Crucial to this multi-layered approach is continuous review requiring rules and thresholds to be adjusted to align with emerging trends in financial crime.³⁴

32 FATF, ‘Guidance on Digital ID’ (March 2020) <<https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html>> accessed 26 January 2026

33 FATF, Guidance on Financial Inclusion (n9)

34 *ibid*

Artificial Intelligence and the Detection of Money Laundering

The growing adoption of AI highlights the dual-use character of technological innovation, particularly as AI is being extensively used both by businesses and by the public. Advances in computing power and big data have significantly expanded the capabilities and accessibility of AI systems. AI may support financial institutions by enhancing transaction monitoring capabilities, strengthening risk detection, and enabling more efficient compliance processes. On the other hand, it may also introduce new vulnerabilities and facilitate more sophisticated forms of financial crime, including through the increased use of deepfakes and other forms of synthetic media.

Prior to the more widespread adoption of AI, financial institutions typically relied on a combination of automated, yet largely static, analyses based on predefined risk factors which were rule-based and then supplemented by human judgement. These approaches often included defensive box-ticking approaches to risk and could only provide a historical view of risk, rather than real-time insight. Furthermore, the lack of more sophisticated technology at the time led to the dependence on humans to analyse large amounts of data which limited the potential to see the more fine-grained picture of risks. Consequently, identification of risk was often delayed, or in some cases undetected, leading to the loss of critical information and limited effectiveness in responding to money laundering threats.³⁵ The rigidity posed by traditional compliance systems created a gap between what the law and FATF recommendations hold and the actual effectiveness of compliance by financial institutions.³⁶

Processing of data and analysis of risk can be aided by AI systems, allowing financial institutions to have an insight into the business relationship quicker and possibly make it easier to identify new risks and emerging methods of money laundering. According to the FATF report of 2021 on 'Opportunities and Challenges of New Technologies for AML/CFT' ('2021 FATF New Technologies Report'), even if conclusions generated by AI systems are the same as those reached by human agents, the combination of human judgement and technological validation of results can enhance institutional confidence in the assessment outcomes. Furthermore, automated risk assessment tools may offer greater objectivity and be more readily auditable by supervising authorities. In the 2021 FATF New Technologies Report, the FATF highlighted how,

*"New technologies were furthermore described as allowing the information held in internal systems to be more accurate, although a few respondents stressed the importance of constant review and the fact that machine learning implies learning from human actions and decisions, and from existing institutional practices."*³⁷

The prevention of money laundering is a key responsibility and challenge for financial institutions especially with the rising number of digital transactions and complex financial systems. AI is capable of analysing vast amounts of data, identifying patterns and predicting money laundering with high accuracy.

35 FATF, New Technologies Report (n6)

36 C Nie et al, 'AI Application in Anti-Money Laundering for Sustainable and Transparent Financial Systems' <<https://www.arxiv.org/abs/2512.06240>> accessed 30 January 2026

37 FATF, New Technologies Report (n6)

According to the European Union's Artificial Intelligence Act ('EU AI Act'), AI is a "*fast evolving family of technologies*"³⁸ which significantly improves industries as it enhances predictive capabilities, enabling more sophisticated data analysis, and optimising operational processes. AI can support more effective risk identification, transaction monitoring, and customer due diligence, thereby facilitating the application of proportionate, risk-based measures. Therefore, AI can significantly improve the effectiveness of anti-money laundering frameworks and access to regulated financial services. Nevertheless, AI may also expose individuals to risks through biased decision-making, lack of transparency, or the automation of exclusionary outcomes.³⁹

An 'AI system' may be defined as a machine-based system capable of operating with varying degrees of autonomy, implying a degree of independence from direct human control, and of exhibiting adaptiveness following deployment. Designed to pursue explicit or implicit objectives, an AI system processes input data and draws inferences in order to generate outputs. Such outputs may take the form of predictions (for example, risk forecasting), content (such as the generation of text or images), recommendations, or decisions. These outputs are capable of influencing both physical and virtual environments, thereby producing real-world effects.⁴⁰

AI techniques such as machine learning, deep learning and natural language processing ('NLP') allow for the detection of suspicious transactions in real time, which data may aid financial institutions in the detection, prevention and mitigation of money laundering.

Machine learning is a subset of AI which focuses on the development of algorithms, allowing systems to learn from data, recognise patterns and make predictions with minimal to no human intervention. Machine learning can aid in tracking international financial flows and support international mutual legal assistance to reduce international crime – such benefits of AI systems are already being leveraged by Europol and Interpol.⁴¹

Machine learning can be supervised or unsupervised. Supervised machine learning is when data is labelled and categorised hence, for supervised machine learning, the input data is paired with the correct output.⁴² Supervised learning models like decision trees and neural networks learn from historical data and distinguish between legitimate and illegitimate transactions. Decision trees work by making decisions based on the input data; hence they may identify suspicious transactions based on amount, location and time. Neural networks aim to mimic the brain's processes and are useful in detecting non-linear relationships and interactions between features.⁴³

38 Regulation (EU) 2024/1689 (Artificial Intelligence Act), Recital 4, <<https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>> accessed 30 January 2026
Hereinafter referred to as the 'EU AI Act'

39 Ibid, recital 5

40 Ibid, article 3

41 S Lyeonov, Z Kubaščíková, V Draskovic and V Fenyves, 'Artificial Intelligence and Machine Learning in Combating Illegal Financial Operations: Bibliometric Analysis' (2024) *Human Technology* 20(2) 325 <https://www.researchgate.net/publication/386198197_Artificial_intelligence_and_machine_learning_in_combating_illegal_financial_operations_Bibliometric_analysis> accessed 31 January 2026

42 B Olufemi, O Bello and K Olufemi, 'Artificial Intelligence in Fraud Prevention: Exploring Techniques, Applications, Challenges and Opportunities' (2024) 5 *Computer Science and Information Technology Research Journal* 1505 <https://www.researchgate.net/publication/383264952_Artificial_intelligence_in_fraud_prevention_Exploring_techniques_and_applications_challenges_and_opportunities> accessed 30 January 2026
Hereinafter referred to as 'B Olufemi et, AI in Fraud Prevention'

43 ibid

Unsupervised machine learning works with unstructured data and is useful in detecting new trends in financial transactions, helping improve anomaly detection. Clustering, such as '*K-Means*' and '*DBSCAN*', is a type of unsupervised machine learning wherein similar data is grouped together and transactions which do not fit in a cluster can be flagged by the AI system for further investigation due to being different from the norm. The benefit of this is that suspicious transactions are generally inconsistent with other regular transactions.⁴⁴

A subset of machine learning is deep learning. Architectures such as convolutional neural networks ('CNN') and recurrent neural networks ('RNN') enhance the detection of fraud by learning complex financial patterns and user behaviour.⁴⁵ CNNs can detect fraud patterns that may remain undetected by traditional detection methods whereas RNNs can handle sequential data and conduct time-series analysis. These types of neural networks are capable of retaining information from previous inputs and improving their outputs as a result. An example given is in fraud detection wherein fraudulent behaviour is flagged in a series of transactions over different time periods.⁴⁶

NLP is a subset of AI which aims to understand, interpret and manipulate human language hence, it may analyse data such as emails, chats and transaction descriptions to detect suspicious language, keywords and phrases which may indicate money laundering. According to the 2021 FATF New Technologies Report, machine learning and NLP are very beneficial to the detection, prevention and mitigation of money laundering.⁴⁷ NLP may also be used to conduct global internet research through web-scraping tools, enabling the collection of publicly available information relevant to a financial institution's risk assessment and compliance activities.⁴⁸

AI has proven results in the detection of money laundering. There have been various studies as to how AI technologies can help in detection of money laundering, such as the study by Bi et al., which found that a multi-layered approach combining both supervised and unsupervised machine learning was able to enhance detection accuracy whilst maintaining efficiency. The dataset comprised two million financial transactions collected from multiple financial institutions over a 24-month period. In their analysis, Bi et al. reported that the proposed systems achieved a 22.3% improvement in recall while maintaining false positive rates below 3%.⁴⁹

Banks around the world, including Standard Chartered Bank in the UK, are also leveraging AI to track transactions in real time and block any suspicious transactions before completion. CitiBank uses AI to facilitate risk management via transactional and behavioural pattern analysis to flag business relations which require further investigation. Whilst some financial institutions refrain from adopting new technologies such as AI due to the costs of such systems, HSBC has proven that AI technologies decrease time and staff requirements for regulatory procedures which, via AI systems, become more effective and cost-saving. Danske Bank's Estonian branch was charged

44 Ibid

45 O Iguodala and A Oyiborhoro, 'AI-Powered Anti-Money Laundering (AML) and Fraud Detection: Enhancing Financial Security through Intelligent Fraud Detection' (2025) *World Journal of Advanced Research and Reviews*, <https://www.researchgate.net/publication/392235964_AI-Powered_Anti-Money_Laundering_AML_and_fraud_detection_-_enhancing_financial_security_through_intelligent_fraud_detection> accessed 30 January 2026
Hereinafter referred to as, 'O Iguodala et, 2025'

46 B Olufemi et, AI in Fraud Prevention (n42)

47 FATF, New Technologies Report (n6)

48 B Olufemi et, AI in Fraud Prevention (n42)

49 W Bi, TK Trinh and S Fan, 'Machine Learning-Based Pattern Recognition for Anti-Money Laundering in Banking Systems' (2024) 4(11) *Journal of Advanced Computing Systems* 30 <https://www.researchgate.net/publication/389037445_Machine_Learning-Based_Pattern_Recognition_for_Anti-Money_Laundering_in_Banking_Systems> accessed 31 January 2026

with laundering more than €200 billion between 2007 and 2015 due to facilitating high-risk clients' access to the American financial system in Estonia and other former Soviet States. After this scandal, Danske Bank adopted AI technologies to identify suspicious patterns such as, through enhanced transaction monitoring systems using machine learning to spot anomalies, the integration of advanced data analytics, regression-based analytical models to understand money laundering indicators and predict behaviour which points to money laundering and automated reporting and compliance.⁵⁰

AI may help financial institutions in meeting the requirements of anti-money laundering detection, prevention and mitigation even through the adoption of proactive measures. For example, predictive analytics may help financial institutions predict which accounts are more susceptible to money laundering or financial crime risks, enabling the financial institution to intervene at an earlier and possibly more opportune stage. Interventions may include increased monitoring of accounts, more detailed customer due diligence and overall better supervision of the accounts.⁵¹

The deployment of AI can enhance the quality and quantity of customer information, reduce false positives through behavioural and pattern analysis, improve the accuracy and timeliness of reporting to financial intelligence units, and facilitate the identification of emerging threats through large-scale data correlation. Continuous monitoring across the customer lifecycle enables the AI system to support the development of more dynamic and granular customer risk profiles and allow for the detection of risk in real time.⁵² Real-time and large-scale monitoring constitutes a significant advantage of AI-based systems, as it enables financial institutions to promptly identify anomalies—such as unusual transaction values, atypical transaction locations, or transaction patterns that deviate from expected customer behaviour. This, in turn, allows institutions to respond swiftly by blocking transactions where necessary or verifying their legitimacy with the customer, thereby enhancing both the effectiveness of risk mitigation measures and the overall customer experience, while safeguarding the integrity of the financial system.⁵³

Whilst AI tools may automate and facilitate compliance for financial institutions, AI tools should not replace human actors and judgement and should be kept as complementary to the financial institution's systems.

50 AMLWatcher, '7 Use Cases of Artificial Intelligence in Anti-Money Laundering' (2024) < <https://amlwatcher.com/blog/7-use-cases-of-artificial-intelligence-in-anti-money-laundering/> > accessed 31 January 2026

51 B Olufemi et, AI in Fraud Prevention (n42)

52 FATF, New Technologies Report (n6)

53 B Olufemi et, AI in Fraud Prevention (n42)

Technical Challenges in Adopting AI Systems

Whilst AI systems pose significant opportunities in detecting, analysing and mitigating money laundering, adopting such systems is not without its challenges. To strengthen their anti-money laundering initiatives by leveraging the power of AI, financial institutions must update their internal operations and traditional systems to adapt to more sophisticated AI systems and train their staff on the use, benefits and consequences of AI systems.

Challenges which may be posed by the use of an AI system include the output of false, inaccurate and biased results, the training of the AI system with poor quality and quantity of data, clarity and transparency and data security and confidentiality. The output of the AI system is determined by its training data; hence, it is crucial to ascertain that data is of the quality and quantity required. This signifies the importance of retaining a human in the loop and sampling the output of the AI system to ensure the accuracy of the output along with retaining explainable AI systems.

Explainability and transparency are critical in ensuring that the outcome can be explained, understood and accounted for. It is imperative that, in addition to detecting and analysing transactions, the AI system is also capable of providing an explanation as to why such a transaction was flagged as fraudulent and how this conclusion was reached.⁵⁴ In fact, Crisanto et al., have held that,

*"AI also offers unprecedented levels of automation and accuracy in regulatory compliance, including fraud detection and AML/CFT. By analysing vast amounts of structured and particularly unstructured data, AI holds the promise of enhancing customer experiences and contributing to a more inclusive financial system."*⁵⁵

Explainable AI systems and retaining a human in the loop is crucial for financial institutions or third-party AI system providers to be able to demonstrate how the AI system came to its conclusion both to authorities and the affected persons.⁵⁶

The requirements put on financial institutions may deter them from having an in-house AI system due to the costs and complexities which might go into it. However, third-party AI system providers may not be able or willing to provide information into the workings of the AI system thereby increasing the 'black box' paradox which financial

⁵⁴ ibid

⁵⁵ JC Crisanto, CB Leuterio, J Prenio and J Yong, 'Regulating AI in the Financial Sector: Recent Developments and Main Challenges' (2024) *FSI Insights* No 63 <<https://www.bis.org/fsi/publ/insights63.pdf>> accessed 31 January 2026

⁵⁶ N Horobets, O Reznik, V Maliyk, I Vyhivskyi and L Bobrishova, 'Artificial Intelligence Technologies in Banking: Challenges and Opportunities for Anti-Money Laundering in the Context of EU Regulatory Initiatives' (2025) *Journal of Money Laundering Control* <https://www.researchgate.net/publication/392468677_Artificial_intelligence_technologies_in_banking_challenges_and_opportunities_for_anti-money_laundering_in_the_context_of_EU_regulatory_initiatives> accessed 1 February 2026

institutions might face.⁵⁷ In addition to this, third-party AI system providers may not be able to demonstrate the integrity of the training data being used and might expose the financial institutions to cyber risks and vulnerabilities.⁵⁸

07

Regulatory Challenges in Adopting AI Systems

In addition to the technical challenges involving AI systems, there are also regulatory ones. Financial institutions making use of AI systems are to adhere to the numerous laws which apply to their operations and the use of the AI system itself, potentially making such use a regulatory burden.

The use of AI is also envisaged in laws and regulations. Regulation (EU) 2024/1624 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing recognises this in Article 76 which requires that ‘obliged entities’ may adopt decisions influenced by AI systems as long as the data processed is obtained in the course of performing due diligence on customers, due diligence measures are subject to meaningful human intervention to ensure accuracy and appropriateness and the customer obtains an explanation of the decisions reached and may challenge such decisions, unless decisions concern suspicious transaction reporting. On this, Brewczyńska explicitly notes how,

“...it would be rather naïve to believe that Article 76(5)(c) of the AML Regulation will unexpectedly bring a considerable change and lead to transparency of AML/CFT policies and procedures developed by obliged entities.”⁵⁹

Brewczyńska argues that Article 76(5) and its corresponding recital 150 of Regulation 2024/1624 are often in conflict with each other due to the restrictive wording of Article 76(5) in relation to how AI systems may be used in decision-making processes and the broader wording of the recital which implies that AI systems may be used in a freer manner. This inconsistency is another challenge for financial institutions as whilst the intention of the legislator, as shown in the recital, suggests a broad interpretation, the actual law is quite limiting thus potentially creating risk to the business of the financial institution. Furthermore, given that Article 76 only applies to information obtained during due diligence checks, information obtained otherwise, such as through financial intelligence units is left out.⁶⁰

Article 75 of Regulation 2024/1624 on exchange of information in the framework of partnerships for information sharing wherein the human in the loop ideal is echoed in sub-article 4 (g) holds that any information generated through AI, machine learning or algorithms may only be shared when such are subject to adequate human

57 U Turksen, V Benson and B Adamyk, ‘Legal Implications of Automated Suspicious Transaction Monitoring: Enhancing Integrity of AI’ (2024) 25(4) *Journal of Banking Regulation* 359
<https://www.researchgate.net/publication/378009404_Legal_implications_of_automated_suspicious_transaction_monitoring_enhancing_integrity_of_AI> accessed 1 February 2026

58 Basel Committee on Banking Supervision, ‘Newsletter on AI and Machine Learning’ (2022),
< www.bis.org/publ/bcbs_ni27.htm > accessed 1 February 2026

59 M Brewczyńska, 2026 (n5)

60 Ibid

oversight.⁶¹ Although well-intentioned, these articles may leave financial institutions/obliged entities in a bit of a loop given that ‘adequate human oversight’ and ‘meaningful human intervention’ remain undefined and without a minimum procedural baseline, potentially leading financial institutions to take a more defensive approach to compliance and supervision, potentially leading to de-risking. Brewczyńska further suggests that these phrases are applicable to derisking and determining the applicable degree of due diligence measures does not prejudice AI use in other compliance areas.⁶² Referring to the EU AI Act, Brewczyńska notes how under Article 14 thereof, high-risk AI systems are required to be designed in a manner which allows effective oversight by humans whilst in use. Brewczyńska analyses how the wording between the EU AI Act and Regulation 2024/1624 do not align, consequently making the meaning behind these two concepts dissimilar. The concept of ‘intervention’ is further analysed which, in contrast with oversight, may require that financial institutions have a more active and direct involvement in each decision.

The EU AI Act aims to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy AI whilst protecting fundamental rights against the harmful effects of AI systems and supporting innovation. Taking a risk-based approach, the AI Act seeks to establish rules binding on persons involved in the lifecycle of the AI system to ensure that, throughout its lifecycle, an AI system complies with the subject matter of the Regulation.⁶³ Taking the definition of ‘AI system’ under the Act – as discussed above – and the abovementioned articles from Regulation 2024/1624, Brewczyńska argues that the legislation is unclear as to whether financial institutions/obliged entities can rely on AI-generated decisions or only use AI-generated predictions or recommendations as input for human-made decisions. Whilst the former interpretation complements Recital 150, the latter retains the human as the dominant player.

The risk-based approach of the EU AI Act classifies certain AI practices as prohibited. Particularly relevant is Article 5 of the Regulation which prohibits the use of AI systems to carry out risk assessments of natural persons for the purpose of assessing or predicting the likelihood that an individual will commit a criminal offence, where such assessments are based solely on profiling or on the evaluation of personal characteristics or personality traits. Therefore, AI systems must be designed to focus on transactional behaviour, objective risk indicators and contextual factors as a whole. This is particularly important for financial inclusion as the use of AI for risk assessments based solely on profiling or personality characteristics or traits could entrench bias and lead to unfair exclusion from the formal financial system. Nevertheless, as Recital 42 holds that AI systems using risk analytics to assess the likelihood of financial fraud based on suspicious transactions are not covered, also not covered are AI systems supporting human assessments based on objective and verifiable facts linked directly to criminal activity.⁶⁴

61 Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, < <https://eur-lex.europa.eu/eli/reg/2024/1624/oj/eng> > accessed 1 February 2026

62 M Brewczyńska, 2026 (n5)

63 EU AI Act (n38), Articles 1 and 2

64 Ibid, Article 5

The prohibition of Article 5(1)(d) of the EU AI Act is mainly aimed at law enforcement entities however, in its Guidelines on prohibited AI practices under the EU AI Act⁶⁵ the European Commission has clarified that it may also apply to private actors such as financial institutions if AI is used for predicting whether a person might commit a crime. The Guidelines hold that if an obliged entity's risk assessment relies only on data prescribed by law – which data is assumed by the legislator as being objective – then such is not a prohibited practice, however the prohibition applies should data be based solely on individual profiling or personal characteristics. Furthermore, the Guidelines suggest that assessments carried out by private entities/financial institutions in the ordinary course of business do not constitute a prohibited practice under Article 5(1)(d), provided they are not based on disallowed forms of profiling. However, this approach complicates compliance for financial institutions, as it may be difficult to determine ex ante whether an AI-based anti-money laundering tool will be regarded as a lawful risk-assessment mechanism or as a prohibited practice under the AI Act. An additional burden on financial institutions is the fact that the Commission Guidelines are interpretative and non-binding hence the way forward by the enforcers of the law may not completely align with what the Guidelines hold.

A final challenge which will be discussed is on the autonomy and adaptiveness of the AI system and the retention of a human in the loop. Retaining a human in the loop is essential however, the legislators and decision makers must accept that, in line with the defining of 'AI System' under the EU AI Act, AI systems have various degrees of autonomy thus it cannot be excluded that certain decisions are made by it. Furthermore, the EU AI Act also recognises the adaptiveness of AI systems thus, marking them as effective and efficient in learning and alerting financial institutions to illicit money flows and predicting suspicious financial activity which requires further investigation. Legislators and decision makers should take a balanced approach in the use of AI systems for anti-money laundering measures. While the retention of human oversight remains essential in order to ensure a human-centred approach to the use of AI systems, consistent with the protection of fundamental rights, AI should be assessed in a holistic manner that takes account of both its benefits and its limitations. In this context, the deployment of AI tools should be aligned with the FATF Recommendations and the principles of the risk-based approach. Accordingly, both the outputs generated by AI systems and the internal processes of financial institutions should be designed and applied in a manner that is proportionate to identified risks and consistent with the risk-based approach of the FATF.

65 European Commission, 'Guidelines on Prohibited Artificial Intelligence Practices under Regulation (EU) 2024/1689 (AI Act)' <<https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>> accessed 1 February 2026

Conclusion

It may be argued that the relationship between AI, the FATF risk-based approach and financial inclusion is better framed as a governance problem rather than a regulatory one. Although the FATF framework should be understood in a risk-based and proportionate manner, its practical application has frequently resulted in de-risking and financial exclusion due to information asymmetries, compliance uncertainty, and enforcement risk.

AI has the potential to realign regulatory practice with underlying principles by enhancing risk differentiation, supervisory visibility, and institutional confidence in managing higher-risk relationships. Hence, AI reframes the risk-based approach from one characterised by risk avoidance and de-risking to one grounded in proportionate risk management. Financial inclusion should thus not be a competing policy objective, but rather, as a functional outcome of effective anti-money laundering supervision, as inclusion strengthens transaction traceability and reduces reliance on informal and unregulated channels.

The effect of AI on the financial institutions' risk appetite is conditional rather than automatic. While AI systems may enable financial institutions to tolerate higher levels of risk through improved monitoring and earlier intervention, regulatory ambiguity, as discussed above, may reinforce defensive compliance and de-risking. Requirements such as "meaningful human intervention" should therefore be understood as governance variables the design and interpretation of which have direct consequences for proportionality and inclusion.

Risks commonly associated with AI, including bias, opacity, and cybersecurity vulnerabilities,⁶⁶ are shaped both by the technology itself and the regulatory design and supervisory expectations placed on financial institutions. Without clear legal standards and consistent supervisory signalling, safeguards intended to protect fundamental rights may inadvertently undermine both anti-money laundering effectiveness and financial inclusion.

When deployed in a manner consistent with the FATF risk-based approach and supported by clear governance frameworks, supervisory trust, and proportionate oversight mechanisms, AI can enhance the effectiveness of anti-money laundering frameworks while supporting financial inclusion. Rather than replacing human judgement, AI should function as an enabling tool—strengthening supervisory capacity, reducing reliance on blunt exclusionary practices, and allowing financial institutions to manage risk more effectively in an increasingly complex and digitalised financial system.

66 O Iguodala et, 2025 (n45)

