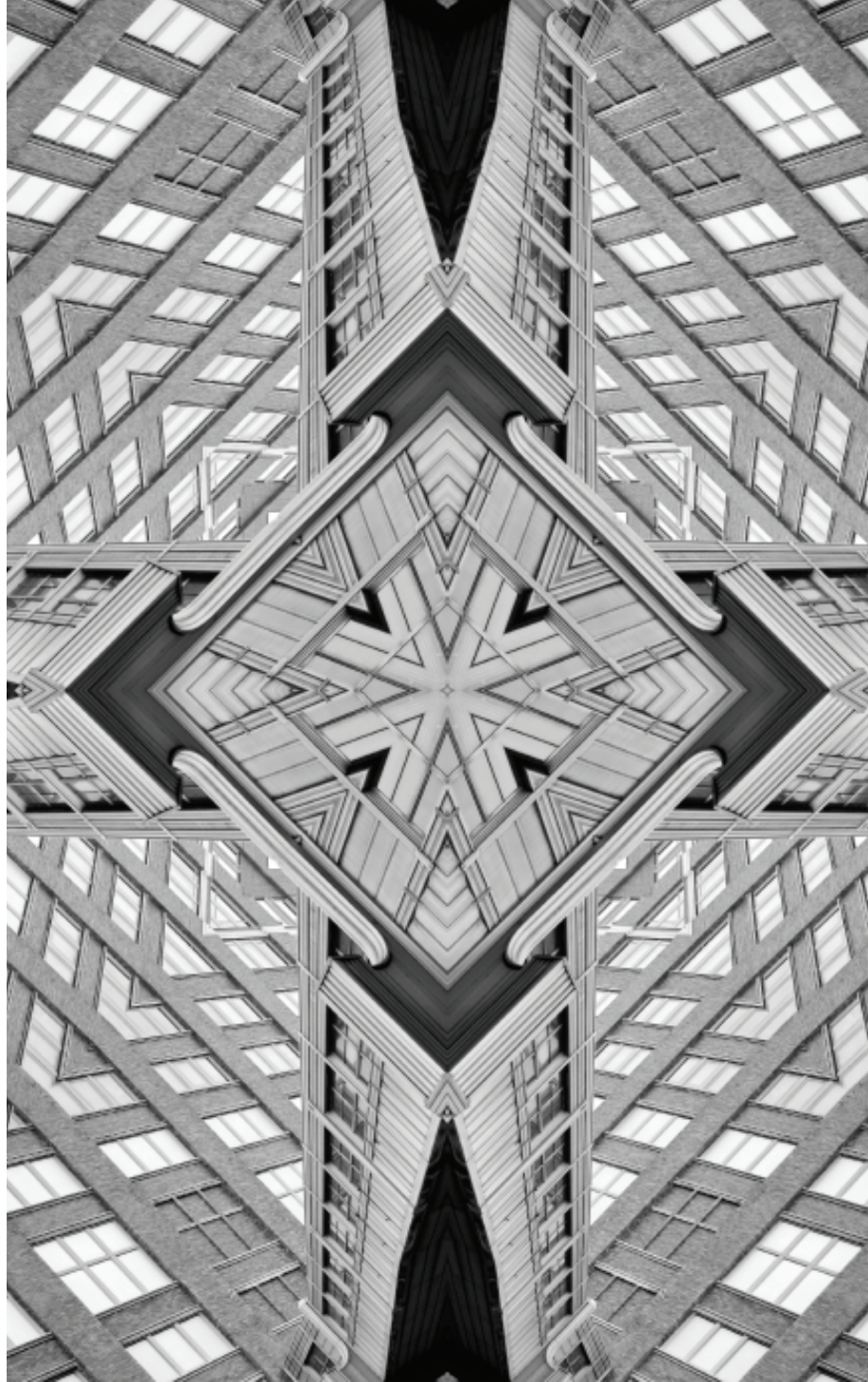


Issue

Brief

ISSUE NO. 726
AUGUST 2024



The Use of AI in Arresting Financial Crime

Sauradeep Bag

Abstract

Artificial Intelligence (AI) is emerging as a promising solution to the challenges of inefficiency and high compliance costs in the fight against money laundering. This brief examines the capabilities, benefits, and challenges of AI in the context of detecting and preventing financial crime. The brief explores the ways in which AI can aid anti-money laundering efforts, particularly by reducing compliance costs and enhancing efficiency. The findings offer insights for policymakers, regulators, and financial institutions seeking to leverage AI to combat money laundering more effectively and efficiently.

Financial criminals work across various platforms, including cryptocurrency exchanges¹ and legitimate enterprises, finding new ways to evade detection and launder their gains. This necessitates a vigilant and more dynamic response to maintain the integrity of financial systems, as traditional anti-money laundering (AML) methods now appear inadequate to address the magnitude of the problem. Artificial Intelligence (AI) has emerged as a potential solution to the inefficiencies in AML practices. The same AI being used to increase the frequency and sophistication of financial crime can improve AML measures.

Typical approaches to detecting financial crimes rely heavily on manual procedures and frequently fall short in the face of the rapid evolution of technology. Despite banks implementing various algorithmic tools to flag suspicious transactions, financial criminals continually adjust their methods to evade detection. This underscores the need for AI and machine learning (ML) applications that can perform real-time analyses of vast datasets to identify patterns indicative of unlawful behaviour.

Institutions like central banks must incorporate and experiment with these emerging technologies. Some private institutions have already begun implementing innovations in AI. Governments can benefit from these pioneering efforts by treating the private sector's advancements as a sandbox for AI adoption and enhancing their own strategies for managing and mitigating financial crime.

The integration of AI-driven AML transaction-monitoring tools is indispensable for financial institutions to stay ahead of evolving threats. These tools detect suspicious activities and continuously refine their algorithms to counter new strategies used by financial criminals. ML technologies, in particular, automate risk assessments, allowing compliance experts to focus their efforts on high-impact activities that demand human judgement and expertise. These technologies mark a shift from reactive to proactive defence, anticipating and neutralising threats before they can inflict damage. Maintaining the sanctity of financial systems requires not just the adoption of new tools but a fundamental rethinking of existing approaches to prioritise agility, foresight, and innovation.

Overview of Money Laundering

Money laundering poses a threat to global financial systems. Criminal organisations, terrorist groups, and corrupt regimes exploit the complexity of the global financial system to launder illicit funds, undermining the integrity of financial markets and threatening global security. Although exact amounts are difficult to quantify, the United Nations Office on Drugs and Crime (UNODC) pegs laundered money between US\$800 billion to US\$2 trillion annually, which is 2-5 percent² of the global GDP.

Governments and international organisations have implemented stringent regulations and frameworks to combat money laundering and terrorist financing. Over the past three decades, there has been a concerted effort to establish complex and sophisticated AML and combating-the-financing-of-terrorism (CFT) frameworks. The European Union (EU) has made progress in this regard through an action plan to combat money laundering and terrorist financing structured around six pillars³ aimed at bolstering the EU's defences and enhancing its global role in combating financial crime.⁴ However, despite these efforts, money laundering remains a persistent challenge, with criminals continuously finding new ways to exploit vulnerabilities in financial systems, highlighting the need for ongoing vigilance and innovation in AML and CFT strategies.

In South Asia, the rapid uptake of online payments and digital wallet technologies has compelled banks and financial institutions to expedite and improve their KYC and transaction monitoring processes. The COVID-19 pandemic further boosted digital transaction volumes, altering customer behaviour and introducing new risks that exacerbate challenges to AML compliance.

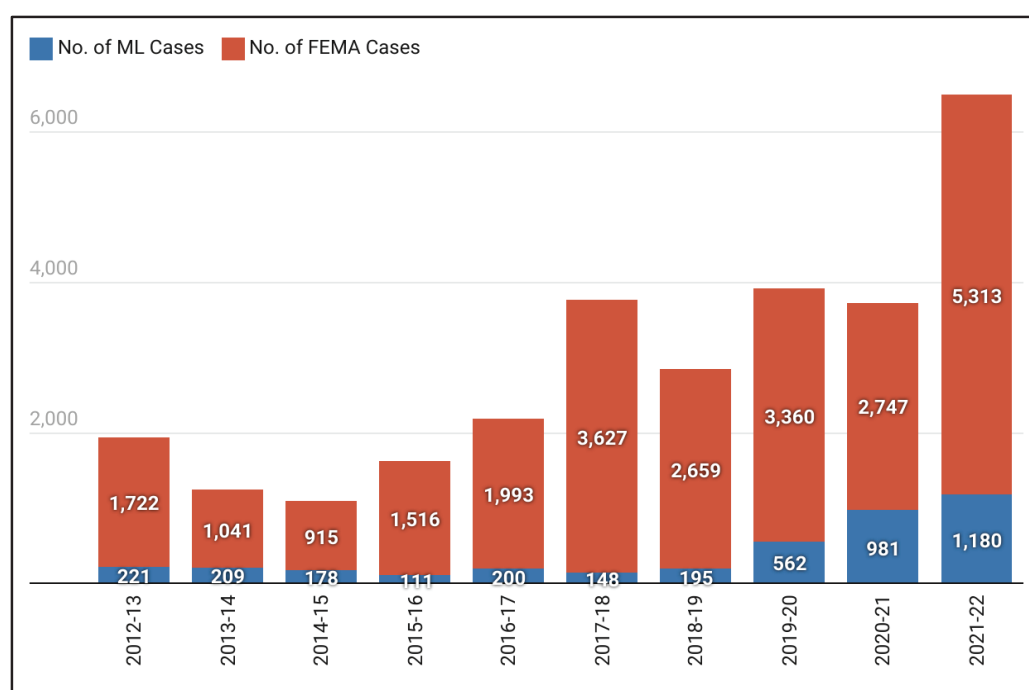
In India, financial crime has evolved to adapt to a complex ecosystem. For instance, a number of payment banks could face regulatory repercussions following the discovery by the Financial Intelligence Unit (FIU) that approximately 50,000 accounts lack proper Know Your Customer (KYC) verification.⁴ These accounts are suspected of being involved in suspicious transactions and potential money-laundering activities. Among these accounts, around 30,000 belong to payment banks other than Paytm Payments Bank.⁵

a The plan includes measures to ensure the effective implementation of existing AML/CFT frameworks, establish a single EU rulebook on AML/CFT, and ensure EU-level AML/CFT supervision. The plan also emphasises the establishment of a support and cooperation mechanism for FIUs, the enforcement of union-level criminal law provisions, and information exchange. It further aims to strengthen the international dimension of the EU's AML/CFT framework. These pillars seek to standardise AML/CFT measures across a single market, enhance supervision and enforcement, and foster cooperation among relevant authorities and institutions.

Overview of Money Laundering

In the past decade, the Enforcement Directorate (ED) recorded its highest number of money laundering and foreign exchange violation cases in 2021 and 2022, with 1,180 and 5,313 complaints, respectively.⁶ From FY 2012-13 to 2021-22, the agency lodged a total of 3,985 criminal complaints under the Prevention of Money Laundering Act (PMLA)⁷ and 24,893 under the civil law of the Foreign Exchange Management Act (FEMA).^{b,8} In the past three years, the ED received over 12,000 complaints around alleged foreign exchange violations.^c Additionally, the adjudicating authority of the PMLA confirmed proceeds of laundering amounting to INR 2,214.92 crore in the last three years.

Figure 1: Money Laundering and Foreign Exchange Management Act Cases in India



Source: Government of India, Ministry of Finance⁹

The question is: Where legislative measures, regulations, policies, tools, and institutional frameworks are falling short, how can emerging technologies like AI aid AML? In order to address this, it is important to understand the challenges faced by the AML ecosystem.

b The ED booked 2,747 cases under FEMA in 2020-21, 5,313 in 2021-22, and 4,173 in 2022-23, totalling 12,233 FEMA cases over the three-year period.

c The number of cases recorded under the PMLA was 981 in 2020-21; 1,180 in 2021-22; and 949 in 2022-23.

The Rise of Financial Crime and India's Response

India has aligned with global efforts to tackle money laundering, drawing inspiration from international agreements such as the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances,¹⁰ the Basel Statement of Principles,¹¹ and the Financial Action Task Force (FATF)¹² recommendations to develop the AML legislation.

The PMLA of 2002¹³ forms the bedrock of the country's AML regulatory framework. This legislation criminalises money-laundering activities and establishes the legal foundation for tracing, seizing, and confiscating proceeds from the crime. One of its key provisions is the requirement for financial institutions and intermediaries to maintain records of specified transactions and report any suspicious activities to authorities. To enforce the PMLA effectively, specialised enforcement agencies such as the ED were established. These agencies are tasked with investigating and prosecuting cases related to money laundering. Additionally, India's AML framework includes the Financial Intelligence Unit-India (FIU-IND), which plays a crucial role in combating money laundering and terrorist financing.

The FIU-IND operates as the repository for receiving cash and suspicious transaction reports (STRs) from financial institutions. It analyses this information to uncover transaction patterns indicative of potential money-laundering activities and shares intelligence with enforcement agencies and regulatory authorities. The FIU-IND has also operationalised an advanced 2.0 version of its information technology system, FINnet. FINnet 2.0 integrates¹⁴ AI and ML tools to improve analytical capabilities, data quality, compliance monitoring, and security. It enables the generation of risk scores for entities and cases, facilitating the identification of high-risk entities for immediate action. It also utilises Natural Language Processing (NLP) and text-mining tools to analyse textual inputs to identify suspicious activities.

The Cost of Compliance

The AML landscape involves numerous stakeholders and significant financial investments from organisations. These investments are essential for the development and maintenance of oversight bodies, financial intelligence units, interconnected databases, and government agencies. Additionally, substantial resources are dedicated to navigating the complex web of regulatory processes, where AML norms, procedures, and technical standards are meticulously formulated, updated, and enforced. As a result, compliance costs for organisations have soared.¹⁵

In a recent study of 1,181 global decision-makers at financial institutions that craft strategies to combat financial crime, several noteworthy trends emerged, propelled by digital transformation, increasingly intricate regulatory environments, and the demand for highly skilled labour.¹⁶ The costs from these factors impact various operational areas significantly. In the Asia Pacific (APAC), the Europe, Middle East, and Africa (EMEA), and the Latin America regions, labour costs in the form of salaries experienced the biggest increase, at 75 percent, 72 percent, and 71 percent, respectively. North America witnessed the greatest increase in technology costs associated with compliance and KYC software, at 78 percent.¹⁷

In addition to human resources, banks have turned to advanced regulatory technology (RegTech) solutions to navigate the complex and evolving regulatory landscape. RegTech has emerged as a critical tool,¹⁸ helping financial institutions to automate and streamline compliance processes, reduce human error, and enhance the detection of suspicious activities. For instance, SymphonyAI¹⁹ is aiding in the analysis of market and operational risks and the detection of potential money-laundering schemes. Initially designed for defence agencies, SymphonyAI has transitioned to the banking sector; the tool reduced false positives in money laundering surveillance for HSBC by 20 percent.²⁰ However, the financial investments required for the implementation and maintenance of these advanced technologies escalate the compliance costs.

Private financial institutions, especially banks, face a formidable challenge in navigating the AML ecosystem, particularly in balancing regulatory adherence and ensuring efficient business operations. Banks are often the first line of defence, tasked with detecting and reporting suspicious activities through comprehensive KYC protocols, which require maintaining detailed records and promptly reporting any unusual transactions to law enforcement agencies. This unique position of banks in financial transactions makes them crucial players in the fight against money laundering and terrorist financing.

Challenges in AML

To meet stringent regulatory requirements, banks are compelled to invest heavily in compliance measures, including hiring several compliance officers. This overhiring significantly increases operational costs. Moreover, the need for continuous training and updating of skills to keep pace with evolving regulations adds to these expenses. However, the effectiveness of banks in detecting and preventing money laundering and terrorist financing remains a subject of debate. While banks are well-positioned to identify fraudulent schemes, the sheer volume and complexity of financial transactions make it challenging to identify all illicit activities. Despite significant investments in compliance measures, the AML ecosystem struggles to keep pace with the evolving tactics of financial criminals.^d

The increasing sophistication of financial crimes necessitates advanced technological solutions as well as a more dynamic and risk-based approach to AML. Financial institutions must move beyond mere box-ticking and embrace innovative strategies that can effectively counter emerging threats. This requires a commitment to continuous improvement and a willingness to invest in both human and technological resources.

“Banks are often the first line of defence in AML, but are challenged by the volume and complexity of financial transactions.”

^d David Lewis, former FATF executive secretary, has been particularly vocal about the inefficiencies within the AML framework. He has criticised the current state of AML efforts as inefficient, highlighting the systemic failures and the need for a fundamental shift in approach. See: <https://www.icij.org/investigations/panama-papers/everyone-is-doing-badly-anti-money-laundering-czar-warns/>

Overcoming Inefficiencies

The effectiveness of AML policies has come under scrutiny due to their seemingly negligible impact on criminal finances. Recent studies²¹ and the UNODC²² suggest that AML interventions manage to seize less than 0.1 percent to around 0.2 percent of laundered proceeds. These findings raise questions about the efficiency of current regulatory systems, especially when criminals continually circumvent them.²³ The data indicates a glaring disparity between policy intent and actual results. If the current system penalises honest entities more than criminal enterprises, it begs the question of its utility. While the clandestine nature of money laundering may make precise estimations challenging, the overarching issue remains: If the primary goal of AML policies is to deter criminal financial activities, the current results suggest a gap between intent and outcome, warranting a re-evaluation of such policies.

Indeed, there is widespread frustration with the global AML landscape, with critics²⁴ highlighting that many governments are more focused on avoiding negative evaluations from the FATF rather than truly addressing money laundering. This fear of landing on the FATF's list of low-scoring countries puts the focus on normative compliance rather than substantive action. This attitude not only undermines the effectiveness of AML policies but also perpetuates a cycle of inadequate enforcement and oversight. If key stakeholders do not prioritise the integrity of the financial system, AML professionals are left to confront a paradoxical situation where their efforts seem futile. AML professionals must take more risks and engage more deeply with the underlying issues of money laundering.

“There is widespread frustration with the global AML landscape.”

Artificial Intelligence and emerging technologies have demonstrated their potential to address an array of challenges across various industries, and they have the potential to offer solutions to the persistent issues in AML and financial crime detection. The rise in crime rates alongside escalating compliance costs, as well as the limited efficiency of existing AML systems, demands a transformative approach. AI could be one of the keys.

AI's ability to analyse large amounts of data rapidly and accurately makes it well suited for detecting suspicious activities and patterns. ML algorithms can learn from historical data to identify new and evolving money-laundering techniques.²⁵ Moreover, AI systems can reduce false positives, allowing investigators to focus on genuine threats and improve the overall efficiency of AML processes. Furthermore, AI can facilitate regulatory compliance by automating the monitoring and reporting of suspicious transactions, thus ensuring that financial institutions adhere to AML regulations effectively. By streamlining compliance processes, AI can help reduce the costs associated with manual oversight and reporting.

The implementation of AI, however, should be accompanied by careful considerations regarding data privacy, security, and ethics. Nonetheless, AI presents a compelling opportunity to address growing challenges in combating financial crimes and enhancing the integrity of the global financial system.

Moving from a Rule-Based System to AI

Rule-based AML systems²⁶ serve as the initial filter to detect suspicious transactions. These systems rely on predefined rules and thresholds, utilising statistical tools like averages and standard deviations to identify transactions that deviate from normal patterns. In practice, rule-based AML systems involve setting up a series of 'if-then' conditions. For example, if a transaction exceeds a specified amount or if multiple transactions occur within a short timeframe, the system generates an alert for further investigation. By analysing transaction attributes such as type, amount, description, time, and location, these systems can flag potentially illicit activities for further investigation.

Yet, rule-based systems have limitations.²⁷ They can generate a large number of false positives, where legitimate transactions are incorrectly flagged as suspicious. This can lead to an increased workload for compliance teams as they sift through alerts to determine which ones require action. Additionally, rule-based systems may struggle to adapt to new or evolving money-laundering techniques, as they rely on fixed rules that may not capture emerging patterns of illicit behaviour.

Financial institutions are increasingly turning to advanced technologies like AI and ML to address these challenges. These technologies have the potential to enhance the effectiveness of AML systems by improving accuracy in identifying suspicious transactions and reducing false positives. They can also provide greater flexibility to adapt to changing threats, making them valuable tools in the battle against financial crime.

The Capabilities of AI

Table 1
Potential Uses of AI in AML

Use	Description
Pattern Recognition	AI and ML algorithms can analyse large volumes of transaction data to identify complex patterns and anomalies that may indicate money laundering or terrorist financing activities.
Behavioural Analysis	By analysing historical transaction data and customer behaviour, AI can create profiles of typical behaviour and flag any deviations from these patterns for further investigation.
Natural Language Processing (NLP)	NLP algorithms can be used to analyse unstructured data to identify suspicious activities or communications related to money laundering or terrorist financing.
Risk Scoring	AI can assign risk scores to customers or transactions based on various factors, such as transaction history, geographic location, and the parties involved, to prioritise high-risk cases for investigation.
Network Analysis	AI and ML can analyse connections between different entities, such as individuals, organisations, and accounts, to identify complex networks involved in money laundering or terrorist financing schemes.
Transaction Monitoring	AI systems can continuously monitor transactions in real time, flagging any suspicious activities for immediate review by compliance teams.
Regulatory Compliance	AI can help financial institutions comply with AML and TF regulations by automating the process of identifying and reporting suspicious transactions, thus reducing the risk of regulatory fines.

Source: Author's own, using various open sources.

The use of AI in AML has shown promising results. One notable example is the partnership between Google and HSBC,²⁸ where AI is being utilised to enhance customer service and streamline operational processes. HSBC has also collaborated with Google Cloud to develop and deploy an AI solution, the Anti Money Laundering AI (AML AI), that is capable of autonomously identifying suspicious activities without specific instructions.^e The Google and HSBC AI AML experiment offers solutions, such as reducing false positives and enhancing the efficiency of identifying suspicious activities.

AI can be further integrated into AML processes by comprehensively understanding behaviour through experimentation and hypothesis testing, which is the approach that Oracle²⁹ has adopted through its Financial Services Compliance Agent, an AI platform for financial institutions. This tool enhances transaction monitoring systems by deploying an AI money launderer in a simulated environment. By running cost-effective experiments and testing hypotheses, the Compliance Agent helps institutions evaluate controls and products within their transaction monitoring systems. It also evaluates system robustness against AI money laundering scenarios, quantifies performance using tailored metrics, and offers evidence-based recommendations for optimising the AML process.

Standard Chartered and Silent Eight^{f,30} are also leveraging AI to enhance their financial crime compliance (FCC) efforts. One of their key initiatives is screening optimisation, which applies ML and NLP to improve name-screening processes against watchlists. By analysing historical case decisions, the Silent Eight engine replicates human analyst assessments, providing true- or false-match recommendations along with written explanations. This approach is aimed at replicating analyst actions, reducing review times, and improving case quality. The continual learning aspect ensures that the algorithms evolve over time to enhance recommendation quality.

e AML AI was trained on a large dataset of customer information to enhance the detection of suspicious activity; the AML AI can identify two to four times more suspicious activity compared to the previous system, while reducing the number of false alerts by 60 percent, based on a comparison of the 12 months following go-live and the preceding 12 months of rule-based monitoring, accounting for seasonality and removing the first month of data after go-live to avoid influencing the result due to detection backlogs. These capabilities allowed investigation teams to focus on genuine cases, resulting in a twofold increase in the identification of financial crimes. AML AI has also reduced processing time and minimised false positives to identify suspicious accounts within eight days after the initial alert. It is also able to recognise established money-laundering patterns, such as rapid fund transfers or sudden activity changes. This capability extends beyond individual detection, enabling the identification of criminal networks collaborating to launder money—an area where rule-based systems have historically struggled.- <https://cloud.google.com/blog/topics/financial-services/how-hsbc-fights-money-launderers-with-artificial-intelligence>.

f A Singapore-based RegTech company specialising in AI for financial crime detection.

Recent Developments

Evidently, banks are actively identifying and addressing gaps in their systems by incorporating technological solutions to combat financial crimes. This underscores the importance for governments and regulators to similarly adapt and monitor the rapid development and integration of emerging technologies in the financial sector.

“AI can be further integrated into AML processes by comprehensively understanding behaviour through experimentation and hypothesis testing.”

The integration of AI into AML practices could revolutionise the detection and prevention of financial crimes. However, this transition is not without its challenges.

The Black Box Problem

The “black box” problem³¹ in AI refers to the challenge of understanding and interpreting the decisions made by complex machine learning models. These models, especially deep learning neural networks, can be intricate and have millions of parameters, making it difficult for humans to comprehend how they arrive at a particular outcome. This lack of transparency raises concerns about accountability, trustworthiness, and ethical implications in AI systems.

One of the main issues with black-box AI models is the inability to explain why a specific decision is made. This lack of interpretability can be problematic, especially in critical applications such as healthcare, finance, and criminal justice, where understanding the reasoning behind a decision is crucial. Without transparency, it becomes challenging to verify the fairness, biases, or potential errors in these models, raising questions about their reliability and accuracy.

For instance, an AI AML system could assign risk scores to transactions or customers. However, the system needs to provide a clear explanation of how it arrived at those scores to help compliance officers understand and justify the decisions made by the AI. Additionally, the AI system used for AML could be trained on historical data that may contain biases. As a result, the system may disproportionately flag transactions or customers from certain demographics or regions as suspicious without providing a clear explanation for these decisions. This can perpetuate existing biases and lead to the unfair treatment of certain groups.

Threats of Generative AI

Generative AI poses a significant risk in AML efforts as it enables criminals to execute complex schemes that can evade traditional detection methods. A concern is the automation and optimisation of money laundering processes, which can make it challenging for financial institutions to identify and prevent illicit activities.

Challenges to AI Integration

The ability of generative AI to create realistic transactions that mimic legitimate financial activities poses a key risk. Criminals can use this technology to split large sums of illegal money into smaller transactions across multiple accounts, obscuring the origin of the money and complicating tracing efforts. Additionally, generative AI can produce convincing invoices, contracts, and other documents to simulate business activities, further blurring the lines between legitimate and fraudulent transactions.

Another risk is the exploitation of online platforms and cryptocurrencies. Criminals can use AI-generated product listings on e-commerce sites to facilitate fraudulent transactions. Similarly, in cryptocurrency, AI-driven transactions can hide money-laundering activities as legitimate trading, which can pose challenges for regulators.


Generative AI can also generate convincing phishing emails and messages, deceiving individuals into unwittingly participating in money-laundering schemes. It can also create artificial identities for credit fraud, allowing criminals to apply for credit or loans by bypassing traditional verification methods.

To counter these risks, financial institutions must deploy advanced detection systems that are capable of identifying suspicious patterns and activities generated by AI. Enhanced monitoring and verification processes are essential for detecting and preventing money laundering schemes that utilise generative AI. Additionally, raising awareness and implementing proactive measures are crucial for mitigating these threats and protecting the integrity of the financial system.

As the application of AI in AML evolves, regulators and financial institutions must implement strong controls and monitoring mechanisms to mitigate existing risks. It is also important for regulators and individuals to monitor these developments closely to protect themselves. Consequently, the integration of AI into AML must be approached with caution, balancing its threats against the opportunities. This area requires further research and understanding, necessitating the allocation of capital to research projects and talent development. Therefore, conducting thorough risk assessments to understand the potential impact of AI integration on AML policies is imperative. Identifying and mitigating risks related to data privacy, security, bias, and explainability to maintain the integrity of AML processes should be the primary focus. Risk assessments must be complemented by continuous monitoring and auditing, implementing mechanisms to detect and mitigate emerging risks and establish regular reviews by independent third parties to ensure compliance and effectiveness.

It is crucial that AI integration into AML policies aligns with existing regulatory frameworks. Thus, developing guidelines that define the permissible scope of AI use, data-handling practices, and transparency requirements to comply with AML laws and regulations must be created with the collaboration of multiple stakeholders. Broadly, the advancement and influence of AI has received scrutiny. It is crucial for stakeholders to remain vigilant about the “unknown unknowns” of AI, i.e., unidentified information that individuals or organisations may recognise as relevant but whose specifics lie beyond current awareness. It is important to approach the development of AI with caution and avoid falling for “AI washing” in various industries. The focus should be on implementing feasible and practical strategies rather than making exaggerated claims about the impact of AI.

Integrating AI into AML could enhance AML efforts, but it is not the end goal. Continued efforts are necessary until such integrations become mainstream. In its current form, maintaining human oversight of AI systems to ensure accountability and ethical use is paramount, from providing regular training to AML professionals on AI technologies, to understanding their limitations.

AI-enhanced techniques can enable AML compliance programmes to be more predictive, efficient, and scalable than traditional rule-based and manual methods. In this context, encouraging financial institutions, regulators, and AI developers to share best practices, insights, and technological advancements in AML to foster a culture of information-sharing and enhance the effectiveness of AI can help combat financial crime. 

Sauradeep Bag is Associate Fellow, ORF.

- 1 United Nations Office on Drugs and Crime (UNODC), “Money laundering through cryptocurrencies,” <https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/laundryingproceeds/moneylaundering.html>
- 2 United Nations Office on Drugs and Crime (UNODC), “Money Laundering,” <https://www.unodc.org/unodc/en/money-laundering/overview.html>
- 3 EUCRIM, “Action Plan on Preventing Money Laundering: Six Pillars,” August 3, 2020, <https://eucrim.eu/news/action-plan-preventing-money-laundering-six-pillars/>
- 4 Pooja Yadav, “After RBI’s Paytm Clampdown, More Payments Bank Under Lens On KYC Worries,” *Inc42*, Feb 16, 2024, <https://inc42.com/buzz/after-rbis-paytm-clampdown-more-payments-bank-under-lens-on-kyc-worries/>
- 5 Yadav, “After RBI’s Paytm Clampdown, More Payments Bank Under Lens On KYC Worries”
- 6 “ED Registered Maximum Money Laundering FEMA Cases During 2021-22 Fiscal: Govt Data,” *TheWeek*, July 25, 2022, <https://www.theweek.in/wire-updates/business/2022/07/25/del77-lsq-ed-cases.html>
- 7 The Prevention of Money-Laundering Act, 2002, Government of India, 2003, <https://enforcementdirectorate.gov.in/sites/default/files/Act%26rules/THE%20PREVENTION%20OF%20MONEY%20LAUNDERING%20ACT%2C%202002.pdf>
- 8 Foreign Exchange Management Act of 1999, Government of India, https://liddashboard.legislative.gov.in/sites/default/files/A1999-42_0.pdf
- 9 Unstarred Question Number 1338, Government of India, Ministry of Finance, Department of Revenue, July 25, 2022, <https://sansad.in/getFile/loksabhaquestions/annex/179/AU1338.pdf?source=pqals>
- 10 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988, https://www.unodc.org/pdf/convention_1988_en.pdf
- 11 Basel Core Principles, <https://www.bis.org/fsi/fsisummaries/bcps.htm>
- 12 Financial Action Task Force (FATF), <https://www.fatf-gafi.org/en/home.html>
- 13 The Prevention of Money-Laundering Act, 2002, Government of India, 2003, <https://enforcementdirectorate.gov.in/sites/default/files/Act%26rules/THE%20PREVENTION%20OF%20MONEY%20LAUNDERING%20ACT%2C%202002.pdf>
- 14 “Financial Intelligence Unit Arms Itself with AI, ML Tools to Check Money Laundering,” *The Economic Times*, May 5, 2024, <https://economictimes.indiatimes.com/tech/technology/financial-intelligence-unit-arms-itself-with-ai-ml-tools-to-check-money-laundering/articleshow/109860949.cms?from=mdr>

- 15 “Rising AML Compliance Costs to Impact Financial Institutions Significantly,” *FinTech Global*, October 3, 2023, <https://fintech.global/2023/10/03/rising-aml-compliance-costs-to-impact-financial-institutions-significantly/#:~:text=Rising%20AML%20compliance%20costs%20to%20impact%20financial%20institutions%20significantly,-October%203%2C%202023&text=It%20has%20been%20uncovered%20that,with%20the%20impending%20AML%20legislation>
- 16 “True Cost of Financial Crime Compliance Study,” *Forrester*, November, 2023, <https://risk.lexisnexis.com/global/en/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report>
- 17 Financial Crime Compliance Costs Rise in Asia, *Finews Asia*, March 6, 2024, <https://www.finews.asia/finance/41017-lexis-nexis-financial-crime-compliance-costs-banking-apac>
- 18 Deloitte, “RegTech – Gaining Momentum: Driving Efficiency in Risk and Compliance,” March 2023, <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-RegTech-Gaining-momentum-noexp.pdf>
- 19 SymphonyAI, <https://www.symphonyai.com/>
- 20 Mark Speyers, “Anti-Money Laundering and AI at HSBC,” *SymphonyAI*, June 1, 2017, <https://www.symphonyai.com/resources/blog/financial-services/anti-moneylaunderinghsbc/>
- 21 Ronald Pol, “Anti-Money Laundering: The World’s Least Effective Policy Experiment? Together, We Can Fix It,” *Policy Design & Practice* Vol. 3, February 2020, <https://www.tandfonline.com/doi/full/10.1080/25741292.2020.1725366>
- 22 United Nations Office on Drugs and Crime (UNODC), “Money Laundering”
- 23 EUROPOL, “The Other Side of the Coin: An Analysis of Financial and Economic Crime,” Publications Office of the European Union, Luxembourg, 2023, <https://www.europol.europa.eu/cms/sites/default/files/documents/The%20Other%20Side%20of%20the%20Coin%20-%20Analysis%20of%20Financial%20and%20Economic%20Crime%20%28EN%29.pdf>
- 24 David Lewis, Speech at the Chatham House Illicit Financial Flows Conference, March 1-2, 2021, <https://www.fatf-gafi.org/en/publications/Fatfgeneral/Chatham-house-march-2021.html>
- 25 Deloitte, “The Case for Artificial Intelligence in Combating Money Laundering and Terrorist Financing,” <https://www2.deloitte.com/mm/en/pages/financial-advisory/articles/the-case-for-artificial-intelligence-in-combating-money-laundering-and-terrorist-financing.html>
- 26 Luigi Bellomarini, Eleonora Laurenza, and Emanuel Sallinger, “Rule-based Anti-Money Laundering in Financial Intelligence Units: Experience and Vision,” *Declarative AI 2020*, July 2020, <https://ceur-ws.org/Vol-2644/paper40.pdf>

Endnotes

- 27 A.N. Bakry et al., “Automatic Suppression of False Positive Alerts in Anti-Money Laundering Systems Using Machine Learning,” *J Supercomput* 80, 6264–6284 (2024), <https://doi.org/10.1007/s11227-023-05708-z>
- 28 Google Cloud, “Fighting Money Launderers with Artificial Intelligence at HSBC,” November 30, 2023, <https://cloud.google.com/blog/topics/financial-services/how-hsbc-fights-money-launderers-with-artificial-intelligence>
- 29 Oracle, “Financial Crime and Compliance Solutions,” <https://www.oracle.com/in/financial-services/aml-financial-crime-compliance/>
- 30 Standard Chartered, “We’ve partnered with Regulatory Technology firm Silent Eight,” July 9, 2018, <https://www.sc.com/en/press-release/weve-partnered-with-regulatory-technology-firm-silent-eight/>
- 31 Yavar Bathaee, “The Artificial Intelligence Black Box And The Failure Of Intent And Causation,” *Harvard Journal of Law & Technology* Vol. 31, 2018, <https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf>

Images used in this paper are from Getty Images/Busà Photography.



Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. Fax : +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org