3

Leveraging AI to Mitigate Money Laundering Risks in the Banking System

Doron Goldbarsht[*]

3.1 INTRODUCTION

Money laundering involves the transfer of illegally obtained money through legitimate channels so that its original source cannot be traced.[1] The United Nations estimates that the amount of money laundered each year represents 2–5 per cent of global gross domestic product (GDP); however, due to the surreptitious nature of money laundering, the total could be much higher.[2] Money launderers conceal the source, possession, or use of funds through a range of methods of varying sophistication, often involving multiple individuals or institutions across several jurisdictions to exploit gaps in the financial economy.[3]

As major facilitators in the global movement of money, banks carry a high level of responsibility for protecting the integrity of the financial system by preventing and obstructing illicit transactions. Many of the financial products and services they offer are specifically associated with money laundering risks. To ensure regulatory compliance in the fight against financial crime, banks must develop artificial intelligence (AI) about emerging money-laundering processes and create systems that effectively target suspicious behaviour.[4]

'Smart' regulation in the financial industry requires the development and deployment of new strategies and methodologies. Technology can assist regulators, supervisors, and regulated entities by alleviating the existing challenges of anti-money laundering (AML) initiatives. In particular, the use of AI can speed up risk

[*] The author wishes to thank Isabelle Nicolas for her excellent research assistance.

[1] *Black's Law Dictionary* (2009), 1097.

[2] 'Money Laundering', *United Nations Office on Drugs and Crime* (Web Page) <www.unodc.org/unodc/en/money-laundering/overview.html>.

[3] Ana Isabel Canhoto, 'Leveraging Machine Learning in the Global Fight against Money Laundering and Terrorism Financing: An Affordances Perspective' (2021) 131 *Journal of Business Research* 441 at 449.

[4] Ibid, 449.

identification and enhance the monitoring of suspicious activity by acquiring, processing, and analysing data rapidly, efficiently, and cost-effectively. It thus has the potential to facilitate improved compliance with domestic AML legal regimes. While the full implications of emerging technologies remain largely unknown, banks would be well advised to evaluate the capabilities, risks, and limitations of AI – as well as the associated ethical considerations.

This chapter will evaluate compliance with the Financial Action Task Force (FATF) global standards for AML,[5] noting that banks continue to be sanctioned for non-compliance with AML standards. The chapter will then discuss the concept of AI, which can be leveraged by banks to identify, assess, monitor, and manage money laundering risks.[6] Next, the chapter will examine the deficiencies in the traditional rule-based systems and the FATF's move to a more risk-oriented approach, which allows banks to concentrate their resources where the risks are particularly high.[7] Following this, the chapter will consider the potential for AI to enhance the efficiency and effectiveness of AML systems used by banks, as well as the challenges posed by its introduction. Finally, the chapter will offer some concluding thoughts.

3.2 ENFORCEMENT AND DETECTION: THE COST OF NON-COMPLIANCE

The FATF sets global standards for AML, with more than 200 jurisdictions committed to implementing its recommendations.[8] It monitors and assesses how well countries fulfil their commitment through legal, regulatory, and operational measures to combat money laundering (as well as terrorist financing and other related threats).[9] Pursuant to the FATF recommendations, banks must employ customer due diligence (CDD) measures.[10] CDD involves the identification and verification of customer identity through the use of other sources and data. Banks should conduct CDD for both new and existing business relationships.[11] They have a duty to monitor transactions and, where there are reasonable grounds to suspect criminal activity, report them to the relevant financial intelligence agency.[12] Banks must conduct their operations in ways that withstand the scrutiny of customers,

[5] FATF, *The FATF Recommendations* (Report, 2012) 7 <www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>.

[6] FATF, *Opportunities and Challenges of New Technologies for AML/CTF* (Report, 2021) 5 <www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf>.

[7] Ibid, 31.

[8] Doron Goldbarsht, 'Who's the Legislator Anyway? How the FATF's Global Norms Reshape Australian Counter Terrorist Financing Laws' (2017) 45 *Federal Law Review* 127. See also 'About', *FATF* (Web Page) <www.fatf-gafi.org/about/whoweare/#d.en.11232>.

[9] FATF, *The FATF Recommendations*.

[10] Ibid, Recommendation 10.

[11] Ibid, Recommendations 10, 11.

[12] Ibid, Recommendation 20.

shareholders, governments, and regulators. There are considerable consequences for falling short of AML standards.

In a 2021 report, AUSTRAC, Australia's financial intelligence agency, assessed the nature and extent of the money laundering risk faced by Australia's major banks as 'high'. The report highlighted the consequences for customers, the Australian financial system, and the community at large.[13] It drew attention to impacts on the banking sector – including financial losses, increased compliance costs, lower share prices, and increased risk of legal action from non-compliance – as well as reputational impacts on Australia's international economic security.[14]

In this climate of heightened regulatory oversight, banks continue to be sanctioned for failing to maintain sufficient AML controls. In 2009, Credit Suisse Group was fined US$536 million for illegally removing material information, such as customer names and bank names, so that wire transfers would pass undetected through the filters at US banks. The violations were conducted on behalf of Credit Suisse customers in Iran, Sudan, and other sanctioned countries, allowing them to move hundreds of millions of dollars through the US financial system.[15] Also in 2009, Lloyds Banking Group was fined US$350 million after it deliberately falsified customer information in payment records, 'repairing' transfers so that they would not be detected by US banks.[16] In 2012, US authorities fined HSBC US$1.9 billion in a money laundering settlement.[17] That same year, the ING Bank group was fined US$619 million for allowing money launderers to illegally move billions of dollars through the US banking system.[18] The Commonwealth Bank of Australia was fined A$700 million in 2017 after it failed to comply with AML monitoring requirements and failed to report suspicious matters worth tens of millions of dollars.[19] Even after becoming aware of suspected money laundering, the bank

[13] AUSTRAC, *Australia's Major Banks: Money Laundering and Terrorism Financing Risk Assessment* (Report, 2021) <www.austrac.gov.au/sites/default/files/2021–09/Major%20Banks%20ML_TF_Risk%20Assessment%202021.pdf>.

[14] Ibid.

[15] Department of Justice, Office of Public Affairs, 'Credit Suisse Agrees to Forfeit $536 Million in Connection with Violations of the International Emergency Economic Powers Act and New York State Law' (Media Release, 16 December 2009) <www.justice.gov/opa/pr/credit-suisse-agrees-forfeit-536-million-connection-violations-international-emergency>.

[16] Andrew Clark, 'Lloyds Forfeits $350 m for Disguising Origin of Funds from Iran and Sudan' (10 January 2009) *The Guardian* <www.theguardian.com/business/2009/jan/10/lloyds-forfeits-350m-to-us>.

[17] Associated Press, 'HSBC to Pay $1.9b to Settle Money-Laundering Case' (11 December 2012) *CBC News* <www.cbc.ca/news/business/hsbc-to-pay-1-9b-to-settle-money-laundering-case-1.1226871>.

[18] Toby Sterling and Bart H Meijer, 'Dutch Bank ING Fined $900 Million for Failing to Spot Money Laundering' (4 September 2018) *Reuters* <www.reuters.com/article/us-ing-groep-settlement-money-laundering-idUSKCN1LK0PE>.

[19] AUSTRAC, 'AUSTRAC and CBA Agree $700 m Penalty' (Media Release, 4 June 2018) <www.austrac.gov.au/austrac-and-cba-agree-700m-penalty>.

failed to meet its CDD obligations while continuing to conduct business with suspicious customers.[20] In 2019, fifty-eight AML-related fines were issued worldwide, totalling US$8.14 billion – more than double the amount for the previous year.[21] Westpac Bank recently agreed to pay A$1.3 billion fine – an Australian record – for violating the Anti-Money Laundering and Counter-Terrorism Financing Act 2006. Westpac had failed to properly report almost 20 million international fund transfers, amounting to over A$11 billion, to AUSTRAC, thereby exposing Australia's financial system to criminal misuse.[22] In 2020, Citigroup agreed to pay US$400 million fine after engaging in what US regulators called 'unsafe and unsound banking practices', including with regard to money laundering.[23] The bank had previously agreed to a US$97.4 million settlement after 'failing to safeguard its systems from being infiltrated by drug money and other illicit funds'.[24] The severity of these fines reflects the fact that non-compliance with AML measures in the banking industry is unacceptable to regulators.[25] More recently, AUSTRAC accepted an enforceable undertaking from National Australia Bank to improve the bank's systems, controls, and record keeping so that they are compliant with AML laws.[26]

The pressure on banks comes not only from increased regulatory requirements, but also from a marketplace that is increasingly concerned with financial integrity and reputational risks.[27] A bank's failure to maintain adequate systems may have consequences for its share price and its customer base. Citigroup, for example, was

[20] Ibid.

[21] Brian Monroe, 'More than $8 Billion in AML Fines Handed Out in 2019, with USA and UK Leading the Charge: Analysis' (2021) *ACFCS* <www.acfcs.org/fincrime-briefing-aml-fines-in-2019-breach-8-billion-treasury-official-pleads-guilty-to-leaking-2020-crypto-compliance-outlook-and-more/>.

[22] AUSTRAC, 'AUSTRAC and Westpac Agree to Proposed $1.3bn Penalty' (Media Release, 24 September 2020) <www.austrac.gov.au/news-and-media/media-release/austrac-and-westpac-agree-penalty>.

[23] Emily Flitter, 'Citigroup Is Fined $400 Million over "Longstanding" Internal Problems' (7 October 2020) *New York Times* <www.nytimes.com/2020/10/07/business/citigroup-fine-risk-management.html>.

[24] Michael Corkery and Ben Protess, 'Citigroup Agrees to $97.4 Million Settlement in Money Laundering Inquiry' (22 May 2017) *New York Times* <www.nytimes.com/2017/05/22/business/dealbook/citigroup-settlement-banamex-usa-inquiry.html>.

[25] Richard Grint, Chris O'Driscoll, and Sean Paton, *New Technologies and Anti-money Laundering Compliance: Financial Conduct Authority* (Report, 31 March 2017) <www.fca.org.uk/publication/research/new-technologies-in-aml-final-report.pdf>.

[26] AUSTRAC, 'AUSTRAC Accepted Enforceable Undertaking from National Australia Bank' (Media Release, 2 May 2022) <www.austrac.gov.au/news-and-media/media-release/enforceable-undertaking-national-australia-bank>.

[27] Barry R Johnston and Ian Carrington, 'Protecting the Financial System from Abuse: Challenges to Banks in Implementing AML/CFT Standards' (2006) 9 *Journal of Money Laundering* 49.

fined in 2004 for failing to detect and investigate suspicious transactions. The bank admitted to regulators that it had 'failed to establish a culture that ensured ongoing compliance with laws and regulations'. Within one week of the announcement by regulators, the value of Citigroup shares had declined by 2.75 per cent.[28]

It is, therefore, in the best interests of the banks themselves to manage risks effectively and to ensure full compliance with the domestic legislation that implements the FATF recommendations, including by retaining senior compliance staff.[29] Despite the high costs involved, banks have largely expressed a strong commitment to improving their risk management systems to protect their own integrity and that of the financial system – as well as to avoid heavy penalties, such as those detailed above.[30] Yet, while banks continue to invest in their capabilities in this area, they also continue to attract fines. This suggests that the current systems are inadequate for combating financial crime.

The current systems rely on models that are largely speculative and rapidly outdated.[31] Fraud patterns change constantly to keep up with technological advancements, making it difficult to distinguish between money laundering and legitimate transactions.[32] But while emerging technologies can be exploited for criminal activity, they also have the potential to thwart it.[33] AI has proven effective in improving operational efficiency and predictive accuracy in a range of fields, while also reducing operational costs.[34] Already, some banks have begun using AI to automate data in order to detect suspicious transactions. Indeed, AI could revolutionise the banking industry, including by improving the banking experience in multiple ways.[35]

[28] Ibid, 52.

[29] Raghad Al-Shabandar et al, 'The Application of Artificial Intelligence in Financial Compliance Management', in *Proceedings of the 2019 International Conference on Artificial Intelligence and Advanced Manufacturing* (New York: Association for Computing Machinery, 2019).

[30] KPMG, *Global Anti-money Laundering Survey: How Banks Are Facing Up to the Challenge* (2004), cited in Johnston and Carrington, 'Protecting the Financial System', 58.

[31] Howard Kunreuther, 'Risk Analysis and Risk Management in an Uncertain World' (2002) 22 *Risk Analysis* 655, cited in Canhoto, 'Leveraging Machine Learning', 443.

[32] Zhiyuan Chen et al, 'Machine Learning Techniques for Anti-money Laundering (AML) Solutions in Suspicious Transaction Detection: A Review' (2018) 57 *Knowledge and Information Systems* 245.

[33] Grint et al, *New Technologies and Anti-money Laundering Compliance: Financial Conduct Authority*.

[34] Institute of International Finance, *Machine Learning in Anti-money Laundering: Summary Report* (Report, 2018) <www.iif.com/portals/0/Files/private/32370132_iif_machine_learning_in_aml_-_public_summary_report.pdf>.

[35] Praveen Kumar Donepudi, 'Machine Learning and Artificial Intelligence in Banking' (2017) 5 *Engineering International* 84.

3.3 LEVERAGING AI FOR AML

AI simulates human thought processes through a set of theories and computerised algorithms that execute activities that would normally require human intellect.[36] It is, in short, the ability of a computer to mimic the capabilities of the human mind. The technology uses predictive analytics through pattern recognition with differing degrees of autonomy. Machine learning is one of the most effective forms of AI for AML purposes.[37] It can use computational techniques to gain insights from data, recognise patterns, and create algorithms to execute tasks – all without explicit programming.[38] Standard programming, in contrast, operates by specific rules that are developed to make inferences and produce outcomes based on input data.[39] Machine learning initiatives allow AML systems to conduct risk assessments with varying levels of independence from human intervention.[40] Deep learning, for example, is a form of machine learning that builds an artificial neural network by conducting repeated tasks, allowing it to improve the outcome continuously and solve complex problems by adapting to environmental changes.[41] Although there are many machine learning techniques, AI has four main capabilities for AML purposes: anomaly detection, suspicious behaviour monitoring, cognitive capabilities, and automatic robotic processing.[42] The effectiveness of these capabilities depends largely on processing power, the variability of data, and the quality of data, thus requiring some degree of human expertise.

The processes involved in AI can be broadly grouped into supervised and unsupervised techniques. Supervised techniques use algorithms to learn from a training set of data, allowing new data to be classified into different categories. Unsupervised techniques, which often operate without training data, use algorithms to separate data into clusters that hold unique characteristics. Researchers maintain that algorithmic processes have the potential to detect money laundering by classifying financial transactions at a larger scale than is currently possible – and with greater accuracy and improved cost-efficiency.[43]

[36] Ana Fernandez, 'Artificial Intelligence in Financial Services', *Economic Bulletin*, June 2019, 1.

[37] FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 22.

[38] Pariwat Ongsulee, 'Artificial Intelligence, Machine Learning and Deep Learning' (15th International Conference on ICT and Knowledge Engineering, 2017).

[39] Steven S Skiena, *The Algorithm Design Manual* (London: Springer, 2008), cited in Canhoto, 'Leveraging Machine Learning', 443.

[40] Isabel Ana Canhoto and Fintan Clear, 'Artificial Intelligence and Machine Learning as Business Tools: A Framework for Diagnosing Value Destruction Potential' (2020) 63 *Business Horizons* 183, cited in Canhoto, 'Leveraging Machine Learning', 444.

[41] FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 22.

[42] Alessa, *Webinar – An Executive Guide on How to Use Machine Learning and AI for AML Compliance* (Video, 2019) <www.youtube.com/watch?v=k46_UY4DGXU>.

[43] While this chapter is primarily concerned with the adoption of AI by banks for AML purposes, AI is also increasingly relied on by AML regulators. Occurring in parallel with increased regulatory demands, the evolution of AI in regulatory technology promised to improve

3.4 THE SHIFT TO A RISK-BASED APPROACH

One of the most significant obstacles for banks seeking to meet their compliance obligations is the difficulty of appropriately detecting, analysing, and mitigating money laundering risks – particularly during CDD and when monitoring transactions.[44] Currently, transaction monitoring and filtering technology is primarily rule-based, meaning that it is relatively simplistic and predominantly focused on automated and predetermined risk factors.[45] The system operates as a 'decision tree', in which identified outliers generate alerts that require investigation by other parties. Thus, when a suspicious activity is flagged, a compliance officer must investigate the alert and, if appropriate, generate a suspicious matter report.[46]

In order to minimise the costs and time required to investigate suspicious transactions, it is essential to detect them accurately at the first instance.[47] In rule-based systems, the task is made all the more difficult by the high false positive rate of the alerts, which is believed to be above 98 per cent.[48] If risk assessment in low-risk situations is overly strict, unmanageable numbers of false positive identifications can cause significant operational costs.[49] Conversely, if risk assessments are too lax, illicit transactions can slip through unnoticed.[50] These static reporting processes make it difficult to analyse increasingly large volumes of data, making them impractical on the scale required by banks. It has thus become necessary for banks to choose between the efficiency and the effectiveness of their AML processes.

Moreover, the rule-based systems rely on human-defined criteria and thresholds that are easy for money launderers to understand and circumvent. The changing

compliance monitoring, as well as reduce costs, which undoubtedly motivated its uptake. See Hannah Harris, 'Artificial Intelligence and Policing of Financial Crime: A Legal Analysis of the State of the Field' in Doron Goldbarsht and Louis de Koker (eds), *Financial Technology and the Law* (Cham: Springer, 2022); Lyria Bennett Moses and Janet Chan, 'Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability' (2018) 28 *Policing and Society* 806; Douglas W Arner, Janos Barberis, and Ross Buckley, 'FinTech, RegTech, and the Reconceptualization of Financial Regulation' (2017) 37 *Northwestern Journal of International Law and Business* 390.

[44] FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 11.

[45] Institut Polytechnique de Paris, 'More AI, and Less Box-Ticking, Says FATF in AML/CTF Report' (Media Release, 13 July 2021) <www.telecom-paris.fr/more-ai-less-box-ticking-fatf-aml-cft>.

[46] Dattatray Vishnu Kute et al, 'Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering – A Critical Review' (IEEA Access, 2021) 82301.

[47] Ibid, 82301.

[48] McKinsey & Company, *Transforming Approaches to AML and Financial Crime* (Report, 2019) 14 <www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Transforming%20approaches%20to%20AML%20and%20financial%20crime/Transforming-approaches-to-AML-and-financial%20crime-vF.pdf>.

[49] Jingguang Han et al, 'Artificial Intelligence for Anti-money Laundering: A Review and Extension' (2020) 2 *Digital Finance* 213.

[50] Ibid, 219.

https://doi.org/10.1017/9781009334297.006 Published online by Cambridge University Press

patterns of fraud make it difficult for rule-based systems and policies to maintain their effectiveness, thus allowing money laundering transactions to be misidentified as genuine.[51] AML systems are designed to detect unusual transaction patterns, rather than actual criminal behaviour. Rule-based systems thus have the potential to implicate good customers, initiate criminal investigations against them, and thereby damage customer relationships – all without disrupting actual money laundering activities. This is because the systems were designed for a relatively slow-moving fraud environment in which patterns would eventually emerge and be identified and then incorporated into fraud detection systems. Today, criminal organisations are themselves leveraging evolving technologies to intrude into organisational systems and proceed undetected.[52] For example, AI allows criminals to use online banking and other electronic payment methods to move illicit funds across borders through the production of bots and false identities that circumnavigate AML systems.[53]

According to the FATF, implementing a risk-based approach is the 'cornerstone of an effective AML/CFT system and is essential to properly managing risks'.[54] Yet many jurisdictions continue to use antiquated rule-based systems, leading to defensive compliance. To keep pace with modern crime and the increasing volume and velocity of data, banks need a faster and more agile approach to the detection of money laundering. They should reconsider their AML strategies and evolve from traditional rule-based systems to more sophisticated risk-based AI solutions. By leveraging AI, banks can take a proactive and preventive approach to fighting financial crime.[55]

3.5 ADVANTAGES AND CHALLENGES

3.5.1 *Advantages*

New technologies are key to improving the management of regulatory risks. Banks have begun exploring the use of AI to assist analysts in what has traditionally been a manually intensive task to improve the performance of AML processes.[56] In 2018, US government agencies issued a joint statement encouraging banks to use innovative methods, including AI, to further efforts to protect the integrity of the financial

[51] FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 12.
[52] Alessa, *Webinar*.
[53] Richard Paxton, 'Is AI Changing the Face of Financial Crimes and Money Laundering?' (26 August 2021) *Medium* <https://medium.com/@alacergroup/is-ai-changing-the-face-of-financial-crimes-money-laundering-912ce0d168bd>.
[54] FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 13.
[55] Ibid, 13.
[56] Ilze Calitz, 'AI: The Double-Edged Sword in AML/CTF Compliance' (27 January 2021) *ACAMS Today* <www.acamstoday.org/ai-the-double-edged-sword-in-aml-ctf-compliance/>.

system against illicit financial activity.[57] The United Kingdom Financial Conduct Authority has supported a series of public workshops aimed at encouraging banks to experiment with novel technologies to improve the detection of financial crimes.[58] AUSTRAC has invested in data analysis and advanced analytics to assist in the investigation of suspicious activity.[59] Indeed, developments in AI offer an opportunity to fundamentally transform the operations of banks, equipping them to combat modern threats to the integrity of the financial system.[60] And, where AI reaches the same conclusions as traditional analytical models, this can confirm the accuracy of such assessments, ultimately increasing the safeguards available to supervisors.[61] Although machine learning remains relatively underutilised in the area of AML, it offers the potential to greatly enhance the efficiency and effectiveness of existing systems.[62]

3.5.1.1 Improved Efficiency

Incorporating AI in AML procedures can reduce the occurrence of false positives and increase the identification of true positives. In Singapore, the United Overseas Bank has already piloted machine learning to enhance its AML surveillance by implementing an AML 'suite' that includes know-your-customer (KYC), transaction monitoring, name screening, and payment screening processes.[63] The suite provides an additional layer of scrutiny that leverages machine learning models over traditional rule-based monitoring systems, resulting in real benefits. In relation to transaction monitoring, the recognition of unknown suspicious patterns saw an increase of 5 per cent in true positives and a decrease of 40 per cent in false positives. There was a more than 50 per cent reduction in false positive findings in relation to name screening.[64]

[57] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, and Office of the Comptroller of the Currency, *Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing* (3 December 2018).

[58] AUSTRAC, *Annual Report 2020–21* (Report, 2021) 21.

[59] Ibid.

[60] Bob Contri and Rob Galaski, 'How AI Is Transforming the Financial Ecosystem' (2018), cited in Deloitte and United Overseas Bank, *The Case for Artificial Intelligence in Combating Money Laundering and Terrorist Financing: A Deep Dive into the Application of Machine Learning Technology* (Report, 2018) 4.

[61] FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 14.

[62] Mark Luber, cited in Markets Insider, 'Machine Learning and Artificial Intelligence Algorithm Paves New Ways for Anti-money Laundering Compliance in LexisNexis Risk Solutions' Award-Winning Solution' (Media Release, 14 November 2018) <https://markets.businessinsider.com/news/stocks/machine-learning-and-artificial-intelligence-algorithm-paves-new-ways-for-anti-money-laundering-compliance-in-lexisnexis-risk-solutions-award-winning-solution-1027728213>.

[63] Deloitte and United Overseas Bank, *The Case*, 25.

[64] Ibid, 29.

https://doi.org/10.1017/9781009334297.006 Published online by Cambridge University Press

AI has the capability to analyse vast volumes of data, drawing on an increased number of variables. This means that the quality of the analysis is enhanced and the results obtained are more precise.[65] At the same time, utilising AI in AML can increase productivity by reducing staff work time by 30 per cent.[66] By combining transactional data with other information, such as customer profile data, it is possible to investigate AML risks within days. In contrast, traditional methods that review isolated accounts often require months of analysis. Additionally, banks can use AI to facilitate the live monitoring of AML standards, which can also improve governance, auditability, and accountability.[67] Overall, the use of machine learning has resulted in a 40 per cent increase in operational efficiency, reinforcing the notion that investment in AI initiatives may have positive implications for the reliability of AML processes.[68]

3.5.1.2 Reduced Compliance Costs

By leveraging AI, banks have an opportunity to reduce costs and prioritise human resources in complex areas of AML.[69] It has been estimated that incorporating AI in AML compliance procedures could save the global banking industry more than US$1 trillion by 2030[70] and reduce its costs by 22 per cent over the next twelve years.[71] The opportunities for cost reduction and improved productivity and risk management offer convincing incentives for banks to engage AI and machine learning to achieve greater profitability.[72] With increased profits, banks could further improve the accuracy of AML systems and, in the process, advance the goals of AML.[73]

3.5.1.3 Increased Inclusiveness

Digital tools have the potential to increase financial inclusion, promoting more equitable access to the formal financial sector.[74] Customers with less reliable forms of identification – including First Nations peoples and refugees – can access banking services through solutions such as behavioural analytics, which reduces

[65] Fernandez, 'Artificial Intelligence', 2.
[66] Deloitte and United Overseas Bank, *The Case*, 29.
[67] FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 20.
[68] Deloitte and United Overseas Bank, *The Case*, 29.
[69] Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications* (Report, 1 November 2017) 23.
[70] 'Strengthening AML Protection through AI' (July 2018) *Financier Worldwide Magazine* <www.financierworldwide.com/strengthening-aml-protection-through-ai#.YV6BGioRrw4>.
[71] Ibid.
[72] Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services*, 9.
[73] Ibid, 25.
[74] Ratna Sahay et al, 'Financial Inclusion: Can It Meet Multiple Macroeconomic Goals?' (IMF Staff Discussion Note SDN/15/17, September 2015).

the burden of verification to one instance of customer onboarding. Utilising AI makes banks less reliant on traditional CDD, offering enhanced monitoring capabilities that can be used to manage verification data.[75]

3.5.2 *Challenges*

Despite the growing recognition of the potential for AI to improve the accuracy, speed, and cost-effectiveness of AML processes, banks remain slow to adopt these technologies due to the regulatory and operational challenges involved.[76] Significant hurdles to wider adoption persist and these may continue to stifle innovations in AML compliance.

3.5.2.1 Interpretation

The difficulty of interpreting and explaining the outcomes derived from AI technologies is among the main barriers to securing increased support for these tools.[77] The Basel Committee on Banking Supervision has stated that, in order to replicate models, organisations should be able to demonstrate developmental evidence of theoretical construction, behavioural characteristics, and key assumptions; the types and use of input data; specified mathematical calculations; and code-writing language and protocols.[78] Yet artificial neural networks may comprise hundreds of millions of connections, each contributing in some small way to the outcomes produced.[79] Indeed, as technological models become increasingly complex, the inner workings of the algorithms become more obscure and difficult to decode, creating 'black boxes' in decision-making.[80]

In the European Union, the increased volume of data processing led to the adoption of the General Data Protection Regulation (GDPR) in 2016.[81] The

[75] FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 17.

[76] Grint et al, *New Technologies and Anti-money Laundering Compliance: Financial Conduct Authority*.

[77] FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 36.

[78] Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services*, 28.

[79] Erik Brynjolfsson and Andrew McAfee, 'Artificial Intelligence, for Real', *Harvard Business Review: The Big Idea* (July 2017) 10 <https://starlab-alliance.com/wp-content/uploads/2017/09/AI-Article.pdf>.

[80] Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services*, 26.

[81] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1. See Christa Savia, 'Processing Financial Crime Data under the GDPR in Light of the 5th Anti-money Laundering Directive', Thesis, Örebro Universitet (2019) <www.diva-portal.org/smash/get/diva2:1353108/FULLTEXT01.pdf>.

https://doi.org/10.1017/9781009334297.006 Published online by Cambridge University Press

GDPR aims to ensure that the data of individuals is protected – particularly in relation to AML procedures, which often collect highly personal data.[82] With respect to AI and machine learning, Recital 71 specifies that there is a right to obtain an explanation of the decision reached after algorithmic assessment. Because regulated entities remain responsible for the technical details of AI solutions, fears persist concerning accountability and interpretability where technologies cannot offer robust transparency.[83] While the GDPR expects that internal compliance teams will understand and defend the algorithms utilised by digital tools, compliance officers working in banks require expertise and resources to do so. It may take a long period of time for even the most technologically literate of supervisors to adjust to new regulatory practices.[84] Efforts to improve the interpretation of AI and machine learning are vital if banks are to enhance risk management and earn the trust of supervisors, regulators, and the public.

3.5.2.2 Data Quality

The data utilised to train and manage AI systems must be of high quality.[85] Machine learning models are not self-operating; they require human intervention to ensure their optimal functioning.[86] In other words, machines cannot think for themselves. Rather, they merely execute and learn from their encoded programming.[87] Since machine learning is only as good as its input, it is crucial that the models used are based on relevant and diverse data.[88] Where money-laundering transactions have not previously been identified by the system, it may be difficult for machine learning to detect future instances.[89] Moreover, false positives would be learned into the system if the training data included them.[90] Therefore, it is essential that data quality is monitored on an ongoing basis to ensure thorough data analysis and regular data cleansing. This serves to highlight the vital importance of vigilant human collabor-

[82] Savia, 'Processing Financial Crime Data'.
[83] Penny Crosman, 'Can AI's "Black Box" Problem Be Solved?' (1 January 2019) *American Banker* 2.
[84] FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 36.
[85] Ibid, 41.
[86] Alessa, *Webinar*.
[87] Lyria Bennett Moses, 'Not a Single Singularity' in Simon Deakin and Christopher Markou (eds), *Is Law Computable? Critical Perspectives on Law and Artificial Intelligence* (Oxford: Hart, 2020) 207.
[88] Mireille Hildebrandt, 'Code-Driven Law: Freezing Future and Scaling the Past' in Simon Deakin and Christopher Markou (eds), *Is Law Computable? Critical Perspectives on Law and Artificial Intelligence* (Oxford: Hart, 2020) 67.
[89] Ibid, 67.
[90] McKinsey & Company, *Transforming Approaches to AML and Financial Crime*.

ation in the technological implementation of AI to ensure that models are well maintained and remain effective.[91]

3.5.2.3 Collaboration

The inexplicable nature of AI, especially machine learning processes, has sparked concerns that are exacerbated by the lack of data harmonisation between actors and users.[92] Currently, customer privacy rules and information security considerations prevent banks from warning each other about potentially suspicious activity involving their customers. While some customers rely on a single financial services provider for all their banking requirements, criminals often avoid detection by moving illicit proceeds through numerous financial intermediaries.[93] The FATF has reported that intricate schemes involving complex transaction patterns are difficult and sometimes impossible to detect without information from counterparty banks or other banks providing services to the same customer.[94] Nevertheless, the FATF's rules to prevent 'tipping off' support the objective of protecting the confidentiality of criminal investigations.[95]

While data standardisation and integrated reporting strategies simplify regulatory reporting processes, they also raise various legal, practical, and competition issues.[96] It is likely that the capacity of banks to model will continue to be limited by the financial transactions that they themselves process.[97] Moreover, where information is unavailable across multiple entities, some technological tools may not be cost-effective.[98] On the other hand, stronger collaboration may introduce the risk of data being exploited on a large scale.[99] There is as yet no 'model template' in relation to private sector information sharing that complies with AML and data protection and privacy requirements. However, information sharing initiatives are being explored and should be considered in targeted AI policy developments.

[91] Ibid.
[92] FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 38.
[93] FATF, *Partnering in the Fight against Financial Crime: Data Protection, Technology and Private Sector Information Sharing* (Report, July 2022) 12 <www.fatf-gafi.org/media/fatf/documents/Partnering-int-the-fight-against-financial-crime.pdf>.
[94] Ibid.
[95] FATF, *The FATF Recommendations*, Recommendation 21.
[96] Juan Carlos Crisanto et al, *From Data Reporting to Data Sharing: How Far Can Suptech and Other Innovations Challenge the Status Quo of Regulatory Reporting?* (Financial Stability Institute Insights No 29, 16 December 2020) 2.
[97] FATF, *Stock Take on Data Pooling, Collaborative Analytics and Data Protection* (Report, July 2021), 11 <www.fatf-gafi.org/media/fatf/documents/Stocktake-Datapooling-Collaborative-Analytics.pdf>.
[98] FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 41.
[99] Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services*, 31.

3.5.2.4 Privacy

Due to the interconnectedness of banks and third party service providers, cyber risks are heightened when tools such as AI and machine learning are used and stored in cloud platforms. Concentrating digital solutions might exacerbate these risks.[100] These regulatory challenges reinforce the desire to maintain human-based supervisory processes so that digital tools are not replacements but rather aids in the enhancement of regulatory systems.[101] Article 22 of the GDPR provides that subjects of data analysis have the right not to be subject to a decision with legal or significant consequences 'based solely on automated processing'.[102] The FATF also maintains that the adoption of AI technology in AML procedures requires human collaboration, due to particular concerns that technology is incapable of identifying emerging issues such as regional inequalities.[103]

3.5.2.5 Bias

Although algorithmic decision-making may appear to offer an objective alternative to human subjectivity, many AI algorithms replicate the conscious and unconscious biases of their programmers.[104] This may lead to unfairly targeting the financial activities of certain individuals or entities, or it may produce risk profiles that deny certain persons access to financial services. For example, AI and machine learning are increasingly being used in relation to KYC models.[105] Recommendation 10 of the FATF standards requires banks to monitor both new and existing customers to ensure that their transactions are legitimate.[106] Without the incorporation of AI, existing KYC processes are typically costly and labour-intensive.[107] Utilising AI can help evaluate the legitimacy of customer documentation and calculate the risks for banks where applications may seem to be fake.[108] The data input team should ensure that it does not unintentionally encode systemic bias into the models by using attributes such as employment status or net worth.[109] Transactional

[100] Crisanto et al, *From Data Reporting*, 5.
[101] FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 39.
[102] *General Data Protection Regulations*, art. 22.
[103] FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 39.
[104] Ibid, 41.
[105] KYC is an element of CDD that aims to prevent people from opening accounts anonymously or under a false name. See FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 43.
[106] FATF, *The FATF Recommendations*, Recommendation 10.
[107] Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services*, 20.
[108] Ibid, 20.
[109] Finextra, 'Responsible Artificial Intelligence for Anti-money Laundering: How to Address Bias' (Blog, 1 September 2021) <www.finextra.com/blogposting/20830/responsible-artificial-intelligence-for-anti-money-laundering-how-to-address-bias>.

monitoring is less vulnerable to such biases, as it does not involve personal data such as gender, race, and religion. Nonetheless, AI and machine learning algorithms could implicitly correlate those indicators based on characteristics such as geographical location.[110] If not implemented responsibly, AI has the potential to exacerbate the financial exclusion of certain populations for cultural, political, or other reasons.[111] The use of these digital tools may thus lead to unintended discrimination.[112] Such concerns are heightened by the fact that the correlations are neither explicit nor transparent.[113] Therefore, regulators must remain mindful of the need to limit bias, ensure fairness, and maintain controls. The evolving field of discrimination-aware data mining may assist the decision-making processes that flow through information technology to ensure that they are not affected on unjust or illegitimate grounds.[114] It does this by recognising statistical imbalances in data sets and leveraging background information about discrimination-indexed features to identify 'bad' patterns that can then be either flagged or filtered out entirely.[115]

3.5.2.6 Big Data

The term 'big data' refers to large, complex, and ever-changing data sets and the technological techniques that are relevant to their analysis.[116] Policymakers and technical organisations have expressed significant concerns over the potential misuse of data.[117] There are also apprehensions that the lack of clarity around how data is handled may lead to potential violations of privacy.[118] In addition, there are uncertainties surrounding the ownership of data, as well as its cross-border flow.[119] Nonetheless, the primary focus should remain on the *use* of big data, rather

[110] Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services*, 27.

[111] World Bank, *Principles on Identification for Sustainable Development: Toward the Digital Age* (Report, 2021) <https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf>.

[112] Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services*, 27.

[113] Lyria Bennett Moses and Janet Chan, 'Using Big Data for Legal/Law Enforcement Decisions: Testing the New Tools' (2014) 37 *UNSW Law Journal* 672.

[114] Bettina Berendt and Sören Preibusch, 'Better Decision Support through Exploratory Discrimination-Aware Data Mining: Foundations and Empirical Evidence' (2014) 22 *Artificial Intelligence and Law* 180.

[115] Ibid, 180.

[116] Janet Chan and Lyria Bennett Moses, 'Making Sense of Big Data for Security' (2016) 57 *British Journal of Criminology* 299.

[117] Ibid, 314.

[118] FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 43.

[119] Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services*, 37.

than its collection and storage, as issues pertaining to use have the potential to cause the most egregious harm.[120]

3.5.2.7 Liability

The issues discussed above raise questions of liability regarding who will carry the burden of any systemic faults that result in the loss or corruption of data and related breaches of human rights.[121] While artificial agents are not human, they are not without responsibility.[122] Because it is impossible to punish machines, questions of liability are left to be determined between system operators and system providers.[123] This situation can be likened to a traffic accident in which an employee injures a pedestrian while driving the company truck. While the employer and the employee may both be liable for the injuries, the truck is not.[124] These issues enliven questions of causation. Will the use of AI and machine learning be considered a *novus actus interveniens* that breaks the chain of causation and prevents liability from being attributed to other actors?[125] The answer to this question will largely depend on the characteristics of artificial agents and whether they will be considered as mere tools or as agents in themselves, subject to liability for certain data breaches or losses. Despite the impact of automation processes on decision-making, doubts remain as to whether AI uses 'mental processes of deliberation'.[126] Due to the collaborative nature of AI technology and human actors, it is generally assumed that AI is merely an instrument and that accountability will be transferred to banks and developers.[127] Therefore, where supervisors can be considered legal agents for the operation of artificial technology, they may incur liability on the basis of that agency relationship.[128] Alternatively, where system developers are negligent as far as security vulnerabilities are concerned, they may be liable for the harm caused by unauthorised users or cyber criminals who exploit these deficiencies.[129] Thus, supervisors and

[120] US President's Council of Advisors on Science and Technology, cited in Moses and Chan, 'Using Big Data', 647.
[121] Fernandez, 'Artificial Intelligence', 6.
[122] Samir Chopra and Laurence F White, 'Tort Liability for Artificial Agents' in Samir Chopra and Laurence F White (eds), *A Legal Theory for Autonomous Artificial Agents* (Ann Arbor: University of Michigan Press, 2011) 120.
[123] Ibid, 154.
[124] Leon E Wein, 'The Responsibility of Intelligent Artifacts: Toward an Automation Jurisprudence' (1992) 6 *Harvard Journal of Law and Technology* 110, cited in Chopra and White, 'Tort Liability', 121.
[125] Chopra and White, 'Tort Liability', 122.
[126] *Pintarich v Federal Commissioner of Taxation* (2018) 262 FCR 41; [2018] FCAFC 79. This case is relevant to the applicability of judicial review to decisions made by machines.
[127] Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services*, 26.
[128] Chopra and White, 'Tort Liability', 130.
[129] Ibid, 126.

developers have a duty of care to ensure that they take reasonable steps to prevent harm or damage.[130] It is possible that, as a result of its continued advancement, machine learning may eventually be granted legal personhood. Rights and obligations would therefore belong to the technology itself, excusing operators and developers from liability.[131] However, this viewpoint remains highly contested on the basis that AI does not possess 'free will', since it is programmed by humans and has little volition of its own.[132] Banks must not underestimate the importance of these concerns. They should ensure that AI and machine learning are carefully implemented with well-designed governance in place so that risks and liabilities are not unintentionally heightened by the use of new technologies.[133] Strong checks and balances are required at all stages of the development process.[134]

3.5.2.8 Costs

Banks must consider the costs of maintaining, repairing, and adapting new AI systems.[135] While AI models have the potential to improve the cost-efficiency of AML compliance, it may be difficult for banks – especially smaller institutions – to budget for high-level AI solutions.[136] Moreover, there are associated indirect costs that require firms to invest in additional funding – for example, updating existing database systems to make them compatible with new AI solutions and hiring staff with appropriate technical expertise.[137]

3.5.3 *Consideration*

AI and machine learning have the potential to provide banks with effective tools to improve risk management and compliance with regard to AML. However, if these new technologies are not introduced with care and diligence, they could adversely

[130] Ibid, 125.

[131] Samir Chopra and Laurence F White, 'Personhood for Artificial Agents' in Samir Chopra and Laurence F White (eds), *A Legal Theory for Autonomous Artificial Agents* (Ann Arbor: University of Michigan Press, 2011). In Australia, AI has already been granted recognition as an inventor in patent applications, suggesting that there is a cultural shift occurring that challenges assumptions in relation to the influence and abilities of AI. See Alexandra Jones, 'Artificial Intelligence Can Now Be Recognised as an Inventor after Historic Australian Court Decision' (1 August 2021) *ABC News* <www.abc.net.au/news/2021-08-01/historic-decision-allows-ai-to-be-recognised-as-an-inventor/100339264>.

[132] Chopra and White, 'Personhood', 173.

[133] Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services*, 26.

[134] Basel Committee on Banking Supervision, *Revisions to the Principles for Sound Management of Operational Risk* (Report, 2021) 16.

[135] FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 40.

[136] Canhoto, 'Leveraging Machine Learning', 448.

[137] Merendino et al (2018), cited in Canhoto, 'Leveraging Machine Learning', 448.

affect AML systems by introducing greater burdens and risks. Some of the challenges presented by AI are similar to those posed by other technology-based solutions aimed at identifying and preventing money laundering. Machine learning, however, offers a relatively new and unique method of classifying information based on a feedback loop that enables the technology to 'learn' through determinations of probability.[138] Banks can thus analyse and classify information through learned anomaly detection algorithms, a technique that is more effective than traditionally programmed rule-based systems.[139] At the same time, the utilisation of AI can exacerbate the complexity and severity of the challenges inherent in AML compliance, particularly in relation to interpretation and explanation.[140] As discussed above, machine learning algorithms usually do not provide a rationale or reasoning for the outcomes they produce, making it difficult for compliance experts to validate the results and deliver clear reports to regulators.[141] This is particularly concerning for banks, where trust, transparency, and verifiability are of great importance to ensure satisfaction and regulatory confidence.[142] Nonetheless, in the current regulatory climate, it seems almost inevitable that banks will continue to leverage AI for AML compliance.

3.6 CONCLUSION

The traditional framework for AML compliance is largely premised on old banking models that do not adequately keep pace with the modern evolution of financial crime. Traditional rule-based monitoring systems are clearly inadequate to detect the increasingly sophisticated methods and technologically advanced strategies employed by criminals. Banks are burdened with false positives while most money laundering transactions remain unidentified, posing a significant threat to the integrity of banks and the financial system itself. Banks that do not meet their compliance obligations expose themselves to significant pecuniary losses and reputational damage.[143]

The FATF has highlighted the potential of innovative technologies such as AI and machine learning to make AML measures faster, cheaper, and more effective than current monitoring processes. While rule-based algorithms remain relevant, harnessing AI and machine learning holds great promise for increasing the accuracy

[138] FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 22.
[139] Deloitte and United Overseas Bank, 'The Case', 25; Fernandez, 'Artificial Intelligence', 2; FATF, *Opportunities and Challenges of New Technologies for AML/CTF*, 20.
[140] Kute et al, 'Deep Learning', 82313.
[141] Ouren Kuiper et al, 'Exploring Explainable AI in the Financial Sector: Perspectives of Banks and Supervisory Authorities' in Luis A Leiva et al (eds), *Artificial Intelligence and Machine Learning* (Cham: Springer, 2022) 105.
[142] Ibid, 105.
[143] Grint et al, *New Technologies and Anti-money Laundering Compliance: Financial Conduct Authority*.

of risk identification and heightening its efficiency due to the large analytical capacity of these processes. While these initiatives may be costly and risky to implement, they offer an excellent return on investment for banks that seek to strengthen their internal AML regime. The implementation of AI is increasingly recognised as the next phase in the fight against financial crime.

Due to the various regulatory and operational challenges that are likely to arise, banks should approach the adoption and implementation of AI with cautious optimism. They should ensure that sophisticated AI and machine learning models can be adequately understood and explained. To achieve optimal outcomes, these technologies should operate in conjunction with human analysis, particularly in areas of high risk. However, banks should be aware that the emphasis on collaboration between analysts, investigators, and compliance officers with regard to AI technology may introduce its own legal and ethical complications relating to privacy, liability, and various unintended consequences, such as customer discrimination.

In the increasingly complex environment of financial crime and AML regulation, banks should thoroughly consider the advantages and challenges presented by AI and machine learning as they move towards the transformation of risk assessment by leveraging AI to mitigate money laundering risks.