Edward O'Keefe

Jules Carter

Sarah Byrne

Can we keep up with the machines? Stronger and faster artificial intelligence systems require robust risk management practices

Received (in revised form): 4th February, 2022

Edward O'Keefe*
Moore & Van Allen, USA

Jules Carter**
Moore & Van Allen, USA

Sarah Byrne[†]
Moore & Van Allen, USA

Barbara Meeks
Formerly of Moore & Van Allen, USA

John Stoker[‡]
Moore & Van Allen, USA

Randal Shields[§]
Moore & Van Allen, USA

Edward O'Keefe *is the co-head of Moore & Van Allen's Financial Regulatory Advice and Response group. Before joining the firm, Ed served as the Global General Counsel of Bank of America Corporation. Having also headed or served as a senior executive with Bank of America's compliance, technology, human resources and operations functions, Ed's broad experience includes all aspects of investigations, litigation, regulatory compliance, governance, cybersecurity, compensation and risk management. His regulatory compliance practice includes working with clients with respect to the Bank Secrecy Act/Anti-Money Laundering (AML) law, anti-bribery/anti-corruption, resolution planning, stress testing and responding to regulatory inquiries. Prior to Bank of America, Ed served as Deputy General Counsel for Deutsche Bank AG and is nationally ranked in Financial Services Regulation (Compliance) by Chambers and Partners. Managing significant and complex bank issues, Ed's experience ranges from supervisory issues to consent orders. He also understands bank operations, including emerging technologies such as artificial intelligence, on which subjects he has presented at international and national industry conferences. As the chair of the Clearing House Association, the industry association of the largest banks, Ed supported and approved the creation of the Real Time Payments system.*

Jules Carter *focuses on helping institutional clients navigate complex regulatory environments and pursue business strategies that balance innovation with risk awareness. Her financial regulatory experience includes representing financial institution clients in response to regulatory enforcement actions and addressing the supervisory concerns of state and federal banking authorities. Her experience is not limited to remediation efforts, as she also assists bank clients deploying targeted marketing algorithms by reviewing model parameters and highlighting regulatory or reputational risks that could emerge. Jules advises on various legal issues for a range of financial services providers, including globally systemic, regional and community banks, as well as fintech companies, money services businesses and brokerage firms.*

Moore & Van Allen PLLC, 100 North Tryon Street, Suite 4700, Charlotte, NC 28202-4003, USA

**Tel: +1 704-331-1033; E-mail: edwardokeefe@mvalaw.com*

***Tel: +1 704-331-3723; E-mail: julescarter@mvalaw.com*

†Tel: +1 704-331-3794; E-mail: sarahbyrne@mvalaw.com

Journal of Financial Compliance
Vol. 5, No. 4 2022, pp. 294–306

2398-8053

Sarah Byrne *leads the firm's Human Trafficking Pro Bono Project, representing survivors of human trafficking, and assisting organisations with human trafficking prevention and compliance programmes. Sarah's years of experience in representing survivors of sex and labour trafficking led to client demand for institutional training and advice on developing anti-trafficking and survivor support programmes, and compliance with related human rights law and regulation. At the national level, Sarah is a frequent conference speaker and advocate for legislative change in support of trafficking victims. She is a founding member of the National Survivor Law Collective, a national network of trauma-informed lawyers providing legal aid to survivors. Representing MVA as a participating member, Sarah works with the United Nation's Finance Against Slavery and Trafficking (FAST) Initiative to increase survivor access to financial services and guide banks on the Survivor Inclusion Initiative. Sarah, along with MVA's multidisciplinary team, brings a unique human rights focus to companies navigating the emerging legal, regulatory and reputational pressures related to environmental, social and governance (ESG) criteria, offering workforce training, and advice on corporate policy drafting, anti money-laundering processes, supply chains, KYC diligence and corporate disclosures.*

Barbara Meeks *combines nearly 20 years of experience as a leader in-house at Wells Fargo with her extensive knowledge of financial institutions and public companies to advise on a broad range of regulatory, compliance, governance, risk management, investigative and transactional matters. Her practice addresses complex legal challenges, including responding to enterprise-critical regulatory mandates and directives. Barbara provides practical and collaborative legal advice to a range of globally systemic, regional and community banks, as well as fintech, treasury management, payments, insurance and brokerage companies. She has expertise regarding comprehensive capital analysis and review (CCAR), living will requirements, interest rate transition, Bank Secrecy Act, financial reporting and broker–dealer and insurance licensing matters. Barbara previously held numerous leadership positions at Wachovia Corporation and Wells Fargo & Company, where, in her last position she led the Global Commercial Banking Section, providing regulatory and legal support to the company's broad platform of banking, insurance and brokerage activities, both domestically and internationally.*

John Stoker *advises clients on a broad array of prudential banking laws and regulations applicable to their financial products, services and operations and to their strategic transactions and investments. Prior to joining the firm, John served as Associate General Counsel of the Corporate Regulatory Section in Wells Fargo's legal department. He leverages his 15 years of in-house legal experience to assist clients in navigating complex regulatory requirements to meet their business and enterprise strategic objectives.*

Randal Shields *served as Deputy General Counsel for the consumer bank at PNC Financial. Randal managed the legal team that supported all of PNC's consumer banking and loan products, channels and regulatory matters. He provided direct support to the bank's fair lending operations and was the principal counsel to PNC's Chief Customer Officer. In addition, he coordinated consumer bank legal activity for examinations by various regulators, including the Office of the Comptroller of Currency and the Consumer Financial Protection Bureau. He previously served as General Counsel for Fleet Mortgage, and as an Associate General Counsel at Bank of America, where he managed legal teams that supported various loan products and related servicing operations.*

Barbara Meeks

John Stoker

Randal Shields

Abstract

No longer just an issue of isolated enterprise, regulatory or reputational risk for financial institutions, compliance failures are indicators of potential systemic deficiencies that can frustrate the mission and

‡Tel: +1 704-331-1176; E-mail: johnstoker@mvalaw.com

§Tel: +1 704-331-1174; E-mail: randalshields@mvalaw.com

ethical goals of a firm. What is more, compliance failures may impede and compromise a financial institution's ability to deliver core financial products and investments. Recent advancements in data management and computing capacity have ushered in a wave of business technology solutions that rely on the power of artificial intelligence (AI) to transform vast quantities of data into useful business and risk management information. Financial institutions utilise these technologies to predict behaviour, make decisions, identify threats and meet regulatory requirements. An unintended consequence of the proliferation of Big Data and advanced analytics is the concomitant expansion of AI-driven models that tend to amplify social and economic biases. As AI-based technologies expand across compliance and risk management functions, they must be subject to rigorous examination and testing. Robust model governance must be a core component of every financial institution's overall risk management and corporate governance strategies. The extent of a financial institution's model governance must align with the extent and sophistication of its model use. This paper sets out the regulatory trends related to AI in compliance and risk management applications and the risks associated with inadequate data management, over-automation and other risk management oversight failures. The possible adverse outcomes are illustrated by means of a case study relating to the detection of money laundering associated with human trafficking. Recommendations for model risk management and model governance follow.

Keywords: artificial intelligence, AI, human trafficking, model risk management, compliance

BACKGROUND

Compliance landscape

Compliance management in banking changed dramatically following the financial crisis of 2008. New laws such as the Dodd-Frank Wall Street Reform and Consumer Protection Act were passed by the US Congress.[1] The prudential regulatory agencies significantly increased supervision and enforcement of regulatory obligations. At the same time, a new consumer-focused regulator was born in the Consumer Financial Protection Bureau (CFPB). These transformational changes to the financial regulatory framework were undertaken with the aim of preventing a similar crisis from ever occurring again. And, indeed, as one respected publication succinctly noted: '[t]en years later, market participants and other companies across the globe operate in a significantly altered landscape marked by heightened regulatory expectations and punishing compliance costs, increasingly active regulatory and criminal enforcement worldwide . . .'[2]

Regulatory scrutiny zoomed in not only on the core operations of these organisations, but also on their managers and directors. Reform efforts sought to strengthen board oversight, position risk management as a key board responsibility and to establish enhanced supervisory standards for risk management at larger institutions.[3] This regulatory scrutiny, combined with internal demands, required financial institutions to develop robust, workable compliance management programmes that can account for increasingly granular operational and regulatory requirements, as well as monitoring and reporting on compliance with those requirements. As the complexity of this task has increased, institutions are continually seeking more sophisticated risk management capabilities. AI is playing an important role in helping these institutions to manage and analyse large volumes of data.

Algorithms and AI

An algorithm is an encoded procedure — basically, a set of rules — used to analyse and transform selected input into desired output based on mathematical assumptions. They can be used to systematically model trends and make predictions about future outcomes

based on observations about past occurrences. Algorithms are fuelled by data. Traditionally, there have been three major challenges to managing large quantities of data: 'the increased Volume of data, the increased Velocity with which it is produced and processed, and the increased Variety of data types and sources'.[4] Recent developments in computing power and automation are allowing us to better respond to these challenges by expanding our capacity to collect, store, analyse and transfer data.

An individual algorithm is a static set of instructions that carries out a predetermined function upon a predetermined set of triggers. AI, on the other hand, refers to a network of complex and adaptable algorithms working to carry out a target function. AI systems operate by modifying individual algorithms within the network and producing new algorithms when necessary. Capable of responding to variations in the information they encounter and learning to recognise new triggers, AI systems are often used to replicate human decision making. AI is enabling financial institutions to analyse and transform vast amounts of data to facilitate complex decision making. But the use of AI systems can have unintended social, legal and regulatory consequences if not designed, used and monitored appropriately. These unintended consequences of the use of AI — particularly those that exacerbate existing social and economic biases — can proliferate quickly as institutions seek to leverage the power of AI at scale. As a result, AI systems require careful evaluation in development, implementation and use. They also require ongoing validation efforts to avoid reputational, legal and regulatory risk.

REGULATORY TRENDS

For financial institutions, the sheer power of AI to quickly analyse, interpret and learn from data is rivalled only by its versatility. Fraud detection teams may leverage AI to analyse typical charges to customer credit cards to help identify new charges that are inconsistent with prior usage and that may be indicative of fraud, while anti-money laundering (AML) teams may use AI to identify new banking activity that could be associated with money laundering. In other cases, businesses may seek to use AI to evaluate financial data and demographic or behavioural characteristics to create targeted marketing campaigns for their products and services, or to make credit or investment decisions.

If an AI tool is not carefully monitored, the system may autonomously recalibrate fraud detection systems so that they routinely decline legitimate customer transactions, resulting, at a minimum, in customer dissatisfaction and frustration. Poor data management principles could, for instance, result in an AI system incorrectly reading a vendor location of 'CA' as Canada and tagging a transaction as suspicious, rather than correctly reading 'CA' as a reference to California, where the transaction would not have given cause for suspicion. Although it may seem helpful, using an AI tool that is not appropriately risk-reviewed and supplemented by human oversight may result in the incorporation of biased assumptions and lead to illegal discriminatory practices.

Whatever a financial institution's needs may be, there is likely to be some AI-powered system advertised as capable of meeting them faster and more consistently than the institution would otherwise be able to do. With AI deployed in so many contexts, in ways that may affect not only the products and services a customer may be offered, but also the terms on which they are provided, the use of AI was bound to attract the attention of legislators and regulators. Haunted by the risk management failures that contributed to the 2008 financial crisis, law makers are focused intently on understanding how firms manage the risks of AI. Financial institutions should fully expect to

become the target of supervisory and enforcement actions in instances where they have failed to implement a reasonable risk management framework to address the potential risks of AI, particularly in cases where consumers have been discriminated against or otherwise adversely affected.[5]

US policy developments

Recent developments indicate increased regulatory attention on the risks associated with financial institutions' reliance on AI. In the USA, the National Artificial Intelligence Initiative Act of 2020 (the AI Initiative) was passed as an addendum to the National Defense Authorization Act for Fiscal Year 2021 (the NDAA).[6] It provides for a broad coordinated effort to accelerate AI research across the various instrumentalities of the federal government. As part of the AI Initiative, the Director of the Office of Science and Technology Policy is coordinating their efforts on AI with the Department of Commerce, the National Science Foundation and the Department of Energy. They are charged with establishing an Interagency Committee to, among other things, support research on the ethical, legal, environmental, safety, security, bias and other issues associated with the use of AI.[7] In addition, the National Institute of Standards and Technology will be empowered to develop best practices and voluntary standards for trustworthy AI.[8] The standards could include establishing common definitions and characterisations for 'explainability, transparency, safety, privacy, security, robustness, fairness, bias, ethics, validation, verification, interpretability and other properties related to artificial intelligence systems that are common across all sectors …'[9]

The Anti-Money Laundering Act of 2020 (the AMLA) is also part of the NDAA. The AMLA represents the most significant change to the USA's bank secrecy, AML and counter-terrorist financing regime since the USA PATRIOT Act of 2001, and it includes US federal government support for automated compliance processes.[10] It also addresses serious concerns regarding the potential use of AI to commit financial crimes. It contains a provision requiring the Comptroller General of the United States to carry out a study on the role that emerging technologies, including AI, can play in assisting with, and potentially enabling, the laundering of proceeds from human-trafficking activity.

In addition to enacted legislation, there have been other legislative proposals designed to raise awareness of the risks of deploying AI. For instance, H.R. 2231, the Algorithmic Accountability Act of 2019, would have required covered commercial entities to conduct assessments of their use of high-risk systems, including AI, that may contribute to bias and discrimination or that make automated decisions, including by evaluating consumer behaviours.

Concern with the increasing use of AI and its unintended consequences is not limited to the legislative branch. Administrative agencies have also undertaken their own efforts to ascertain the nature and extent of AI usage. In March 2021, federal bank agencies issued an interagency request for information on financial institutions' use of AI and machine learning in the provision of services to customers and for other business or operational purposes.[11] The agencies sought input from financial institutions and private sector stakeholders regarding model governance principles, risk management approaches and control processes that allow financial institutions to deploy AI-enabled systems in a manner consistent with overall safety and soundness.

Specific risks highlighted in the request for information and comment include: an inability to explain how AI arrives at its outcomes; limitations of dataset that AI may use to identify patterns and correlations in generating predictions; and the ability of AI to update itself and evolve without human

interaction.[12] The agencies are expected to use the broad-based input received from the request to inform their views on whether further supervisory clarification would help in aiding financial institutions to use AI in a safe and sound manner.[13]

Non-US developments

Efforts to proactively address the rise of AI usage are not limited to those in the USA. In the EU, the dearth of comprehensive and effectual standards governing the use of data-driven AI models is emerging as an area of major public concern. In April 2021, the European Commission released a proposal for a regulation, also known as the Artificial Intelligence Act, outlining harmonised rules on AI with the goal of 'address[ing] the opacity, complexity, bias, a certain degree of unpredictability and partially autonomous behaviour of certain AI systems, to ensure their compatibility with fundamental rights and to facilitate the enforcement of legal rules'.[14] The act specifically addresses AI systems used by regulated financial institutions, aiming to ensure synchronous and non-duplicative enforcement of the proposed regulations under the Act, along with the relevant rules and requirements under existing EU financial services legislation. In the UK, the Financial Conduct Authority and the Bank of England launched a public and private sector forum in October 2020 to understand the uses and impacts of AI on the UK's financial markets. The forum will hold quarterly meetings focused on data, model risk management and governance.[15]

In Asia, the Monetary Authority of Singapore (the MAS) released a set of principles in late 2018 for the responsible use of artificial intelligence for data analytics (AIDA) in product and services decision making.[16] The MAS cited the heightened potential risk of systemic misuse posed by the increasing prevalence of AIDA, as compared to human decision makers.[17] The principles address the need to ensure individuals or groups are not systemically disadvantaged through decisions made by AIDA; that AIDA usage aligns with the firm's ethical standards, values and codes of conduct; that there is appropriate internal and external accountability for the firm's use of AIDA; and that firms are transparent in their usage of AIDA, what data is used and how it is used, and the consequences of AIDA-driven decisions.[18]

MODEL RISK MANAGEMENT

AI decision making and decision-facilitating systems can be used across an organisation and, therefore, can create true enterprise-wide risk and potentially result in financial losses, reputational damage, strategic decision-making failures and customer harm. As a result, a strong governance framework is essential to ensuring that AI systems are developed, validated, implemented, and used appropriately. In its most recent 'Model Risk Management Handbook', the Office of the Comptroller of the Currency (the OCC) highlights sound AI risk management activities, including: conducting appropriate due diligence and risk assessments when AI is implemented; ensuring the bank has appropriately qualified staff to implement, operate and control risks associated with AI; having an inventory of AI uses across the bank; identifying the level of risk associated with each AI usage; establishing clear parameters for the use of AI; having a process for effectively validating that AI usage results in sound outcomes that are not unfair or biased; and having effective technology controls.[19] A few of the risks associated with AI, and practices to help manage those, are outlined below.

Model development

Before it is put into use, a model must learn to perform its target function through exposure to large volumes of training data. One of the principal sources of model risk is poor

training data management. For example, when a model is trained on data collected in a manner that is inconsistent with applicable law or regulation — or is just wrong — the output will be faulty. Also, when a model is trained on a dataset that is properly collected but does not represent the sector of the population that the model will ultimately be applied to, it will not perform appropriately. For example, it may predict or direct outcomes that harm the intended customers.

Financial institutions must also be aware of the confounding effects of biased training data during the model development phase. This latent bias may originate from cumulative error when attempting to teach a model to recognise 'good' and 'bad' outcomes. If, for example, a suspicious activity detection model is trained on a dataset intended to include genuine transaction information, that data subset may inadvertently include information relating to undiscovered illicit financial activity. In such a case, the model would 'learn' that certain illegal transactions are actually acceptable.

While some potential areas of bias may be clear or easier to identify, institutions should not underestimate the potential for latent bias to influence the development of a full range of decision making across the company, resulting in continued inequality. In a 2018 address on the opportunities and risks of financial institutions leveraging AI, Governor Lael Brainard of the Board of Governors of the Federal Reserve System cited a reported instance of a company using an AI tool to assist in its hiring of software developers. Trained on the CVs of prior appointees, who were overwhelmingly male, the AI tool's learnings led it to exclude the CVs of graduates from two women's colleges.[20] Heightened vigilance is necessary to identify the potential for latent drivers of bias within datasets and also for the possibility that a model developer may view some outcome inequalities in a model as simply natural and acceptable.

Firms should ensure consistent protocols for data collection, processing and structuring, and ensure that the target population is well represented. Training data protocols should address the following: (a) how to identify and document the source and provenance of data; (b) how to make decisions about what data to include or exclude from the training datasets; (c) how to define, and potentially exclude, non-useful outliers; (d) protocols for transforming data in order to make it recognisable to the model.

Another critical area of focus for institutions in AI risk management is ensuring that model development teams do not consist solely of those individuals with sufficient qualifications and the skills needed simply to build the model. The teams must also include business, operations, risk and compliance and legal members who can provide the necessary insight and knowledge to identify and address its potential risks and weaknesses. Model developers may have the mathematical or programming skills necessary to create a model, but it should not be surprising if these technical model builders do not have a full appreciation of the compliance risks, for instance, that a credit decisioning model may generate and how those risks can be identified and mitigated. Institutions should leverage their inventory of AI uses and assess their related risks to determine the overall skill sets and level of input needed to properly assess and manage those risks.

Model supervision

Automated systems often cause human value judgments to be viewed through the veil of abstract computational objectivity, thereby alienating them from institutional accountability structures. But every model is an assemblage of 'institutionally situated code, practices, and norms with the power to create, sustain, and signify relationships among people and data through minimally

observable, semiautonomous action'.[21] And, as with any assemblage of institutional actors, human or non human, there are no substitutes for the value of experienced human decision making. Model supervision failures and overreliance on AI systems as the sole basis for decision making is another critical source of risk.

Human interaction should be a core component at all stages of model development and use. From a corporate governance perspective, roles and responsibilities and lines of reporting within the model risk management framework should be clearly defined by management. Governance should include assigning control groups and model owners, who are ultimately accountable for development, implementation and use of each individual model. Model risk management policies and procedures should also outline the types of functions and decisions that require human corroboration in the form of documentary evidence, certifications, or some other artefact to support decisions that are made primarily based on model output.

Effective model supervision will require more than just the participation of management. Employee training should also emphasise that the human actors are responsible for policing the algorithms, and not the other way around. Employees engaged in the development and implementation of the model should be instructed to assume the fallibility of the model and to flag any issues they notice rather than assuming that the AI system will detect it or that responsibility for identifying issues instead resides with independent risk management or audit functions. This is an important part of creating a culture of compliance across all functions.

Testing and validation

Testing and validation are essential components of model governance. They allow developers to identify instances in which a model is failing to perform its target function. Model risk management policies and procedures should establish standards for testing and validation, including the scope and frequency of those activities, both before models are put into production and on an ongoing basis thereafter. Specifically, financial institutions should establish protocols for periodic evaluation of the conceptual soundness and key underlying assumptions of each model using a variety of analyses. The required frequency of these validation exercises should be determined based on the level of risk inherent in the model itself and accounting for the risk associated with the activities it supports.

The model risk management framework should also account for validation of vendor models and evaluation of data produced using other third-party models. A designated internal party should be responsible for verifying that the agreed upon scope of work has been completed. The same party should evaluate and track identified issues to ensure they are addressed. The responsible party can be an individual, a project team or a department, depending upon the size and applicability of the model. Institutions should ensure that all necessary authority to inspect the models is included in any contracts with third-party vendors, particularly with respect to proprietary third-party technologies.

Internal audit

If a financial institution relies on AI-driven systems, its internal audit function should verify that: (a) model owners and control groups are complying with policies and procedures; (b) validations are performed in a timely manner; (c) models are subject to controls that appropriately account for any weaknesses in validation activities. They should further evaluate processes for establishing and monitoring limits on model usage and determine whether procedures for updating models are clearly documented. Their protocols should include testing whether

evaluation procedures are being carried out as specified and check that model owners and control groups are meeting documentation standards. The process should include reviewing the critical element of risk reporting. Finally, they should perform assessments of supporting operational systems and evaluate the reliability of data used by models.

Record-keeping and documentation

Documentation provides for continuity of operations, makes compliance with policy transparent, and helps track recommendations, responses and exceptions. Failure to promulgate adequate record-keeping policies and procedures, or to apply existing record-keeping protocols to compliance technology solutions, will drastically increase exposure to model risk. Even minor adjustments to a model in response to testing and validation can have major effects on performance. Detailed records must be maintained to enable effective oversight. It is important to ensure adequate record retention to preserve all key artefacts. Documentation of model development and validation should be sufficiently detailed so that parties unfamiliar with a model can understand how the model operates, its limitations, and its key assumptions. The records should include analysis and support for key aspects of the system, including assumptions. Documenting decisions helps improve them through focusing thought and structure.

ADVERSE OUTCOMES ILLUSTRATED BY HUMAN TRAFFICKING

The regulatory trends and risks related to AI can be illustrated through consideration of the use of AI to combat money laundering associated with the crime of human trafficking.[22] This case study reflects the experiences and understanding of both the human-trafficking survivors and AML professionals with whom the authors have consulted, and the observations of the authors who practise in the area of human trafficking prevention and compliance.

Regulatory focus

According to the US Department of the Treasury's 2020 National Strategy for Combating Terrorist and Other Illicit Financing, human trafficking is one of the most significant illicit finance threats facing the USA and its financial systems.[23] Recent and increased regulatory focus on detecting human trafficking in AML processes is clear. In October 2020, the Financial Crimes Enforcement Network of the US Department of the Treasury (FinCEN) released its Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity.[24] The Supplemental Advisory focuses on four evolving tactics used by human traffickers to carry out and hide the proceeds from their illicit operations: front companies, exploitative employment practices, funnel accounts and alternative payment methods.

Separately, and specific to this topic of this paper, the AMLA of 2020 requires that the Government Accountability Office (GAO) conduct studies and report on, among other things, 'the role that emerging technologies, including artificial intelligence . . . and other innovative technologies, can play in assisting with and potentially enabling the laundering of proceeds from trafficking'.[25] On 30th June, 2021, the Office of the Comptroller of the Currency and other agencies issued an interagency statement explaining the new national AML/Combating the Financing of Terrorism priorities as published by FinCEN and other financial regulators in accordance with the AML Act of 2020.[26] The new national priorities include 'human trafficking and human smuggling'. Revised regulations will follow the newly announced priorities. That the regulators included human trafficking in that short list is a clear indicator of anticipated enforcement.

In 2020, Deutsche Bank was fined US$150m by the New York State Department of Financial Services (NYSDFS) for compliance failures related to client Jeffrey Epstein, his sex trafficking enterprise and correspondent banks. In the Consent Order, NYDFS found the Deutsche Bank 'conducted business in an unsafe and unsound manner [and] failed to maintain an effective and compliant anti-money laundering program'. Also in 2020, Westpac Bank was fined US$920m by the Australian Transaction Reports and Analysis Centre (Australia's financial intelligence, AML and counter-terrorism regulator) for failures in AML reporting, record-keeping and detection, including transfers indicative of child sex trafficking. The Westpac fine is the largest paid to an Australian regulator for violation of money laundering laws to date. The increased regulation and enforcement mean that compliance professionals are having to refine their processes, which include reliance on AI.

Use of AI to detect human trafficking

Financial institutions already employ technology to detect human trafficking in financial flows. Typologies that currently prompt AML professional review involve cash deposit and withdrawals, fund transfer size and frequency, account user relationships, payments for certain goods and services and use of virtual currency.[27] Notably, typologies may reflect the behaviour of traffickers, or victims who are forced into financial transactions by traffickers. These typologies, pattern analysis and resulting Suspicious Activity Reports are an important part of law enforcement intervention in human trafficking criminal conduct.[28] The typologies leading to the alerts are manually adjusted based on Suspicious Activity Report results, regulatory guidance and risk tolerance policies.

AI enhances human trafficking detection by auto-refining the typologies based on previous accurate identification. Ideally, monitoring occurs across systems to include transactions involving personal and business bank accounts, prepaid accounts, mobile payment applications, third-party payment processing and wire transfers.[29] AI can include risk profiles based on industry, business types (including inconsistencies in business types and hours of operation) and geography, and it ought to scan for, and learn about, the absence of transactions, including payments for housing and personal care items, or patterns reflecting no payroll or income subsidy of any kind. Use of AI in this space is important due to the ever-increasing volume of unstructured data presented to financial institutions as part of customer due diligence, as well as the increasing regulatory pressures noted above.

Risks in AI

The expansion of AI to detect human trafficking will yield an increase in efficiency for detecting financial crimes. However, while using AI is helpful, relying on it too much, too little or erroneously in AML and account management can pose meaningful risk. Here are examples of adverse outcomes.

Siloed monitoring

AML systems that monitor only at the transaction level in an isolated environment without considering indicators that may exist on other financial institution platforms may be less effective at detecting illicit activity. For example, a system designed to flag indicia of human trafficking such as structuring, that is separating a large transaction into a series of smaller transactions below the applicable reporting threshold, may successfully determine that a series of deposits into the same account should be aggregated for reporting purposes. If, however, the transactions are dispersed across different payment media, such as money orders, wire

transfers, peer-to-peer payment platforms, cryptocurrency exchanges or prepaid accounts, a siloed monitoring system will be insufficient. In addition to the regulatory risk associated with facilitating undetected, apparently illicit financial activity, failure to identify proceeds of human trafficking will also impede later efforts to obtain restitution for victims. Furthermore, even if a financial institution is capable of detecting patterns of illicit financial activity, failure to implement a holistic model to accommodate intra-platform contextual considerations could result in missed detection of victimisation and the unjust termination of a banking relationship without a complete picture of account-holder activities.

Erroneous detection of suspicious activity and de-banking

AI systems can learn to identify suspicious activity and automatically close suspicious accounts without further human intervention. While these systems may be attractive as large-scale risk management tools, they may also have the effect of blacklisting customers flagged as 'high risk'. And because this information is often shared between affiliated financial institutions, an erroneous alert can not only disqualify a person from doing business with the bank that detects the alert, but also affect their ability to access credit, payment systems and financial services at other institutions. Examples of profiles that are erroneously flagged and de-banked include workers in legitimate cash-intensive businesses (eg nail and hair salons, laundromats, bars and restaurants). Similarly, reports show that workers engaged in lawful sex work (eg exotic dancing, escort services, webcam modelling) are often de-banked due to account activity that seems, or is perceived to be, illicit.[30] Exclusion is a reasonable response to suspected fraud or money laundering, but it becomes problematic when applied automatically and erroneously to customers whose legitimate activity resembles suspicious activity, creating barriers to accessing financial services that can directly prompt financial instability and personal suffering.

Many financial institutions use automated systems to decline or close accounts in response to activity indicating account mismanagement, such as a prolonged overdraft. However, this type of automated account closure could cause human trafficking survivors to be prevented from accessing financial services at a time when they are seeking financial recovery and independence. Without due diligence to understand the reason for the account mismanagement and, where appropriate, offering an opportunity to develop financial literacy, an already vulnerable customer may be rendered more vulnerable upon loss of financial services. This is particularly acute for survivors experiencing ongoing financial exploitation resulting from identity theft and delinquent credit.[31]

Regulators are increasingly focused on the evolving tactics of traffickers, behaviours of victims, and use of AI to aid in detection of this crime. To better protect vulnerable customers and mitigate risk to all stakeholders, financial institutions might consider AI improvements designed to identify human trafficking activity in a manner that is both accurate and precise, and to avoid false positives.

CONCLUSION

Effective AI can reduce expense and drive customer satisfaction through consistent and compliant operations. Inadequate AI system design or input that leads to inaccurate or misinterpreted output may not be much different from not receiving any output at all. And, as bankers have come to realise, regulators will not give an institution — even one with a complex AI system — a pass if it fails to accomplish its compliance goals. Thus, AI systems need to be carefully designed, monitored, and augmented. Integration with

existing data systems or with other AI systems can directly assist in accomplishing an institution's mission. In the end, an AI enhanced institution can improve its efficiency and efficacy while avoiding undesirable outcomes such as regulatory enforcement or customer dissatisfaction.

Acknowledgment

The authors would like to thank Barbara Meeks of Chapman and Cutler LLP for her contributions.

References

(1) Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 929-Z, 124 Stat. 1376, 1871 (2010), available at https://www.govinfo.gov/content/pkg/PLAW-111publ203/pdf/PLAW-111publ203.pdf (accessed 10th June, 2022).

(2) Karp, B. (Paul, Weiss, Rifkind, Wharton & Garrison LLP) 'The Financial Crisis 10 Years Later: Lessons Learned' (5th October, 2018), Harvard Law School Forum on Corporate Governance, available at https://corpgov.law.harvard.edu/2018/10/05/the-financial-crisis-10-years-later-lessons-learned/.

(3) See Kevin LaCroix (1st April, 2015), 'Bank Directors Facing Increased Regulatory Scrutiny, Raising Fears of Potential New Liability Exposures', available at https://www.lexisnexis.com/legalnewsroom/corporate/b/blog/posts/bank-directors-facing-increased-regulatory-scrutiny-raising-fears-of-potential-new-liability-exposures; see also 'United Nations Conference on Trade and Development, Corporate Governance in the Wake of the Financial Crisis; Selected International Views' (2010); see also 'Heightened Standards for Large Banks; Integration of 12 CFR 30 and 12 CFR 170: Final Rules and Guidelines', OCC Bulletin 2014-45 (2014) (rescinded); see also Office of the Comptroller of the Currency, Consumer Compliance (CC): Compliance Management Systems, in 'Comptroller's Handbook', Version 1.0 (2018).

(4) Bennett Moses, L. & Chan, J. (2014) 'Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools, *University of New South Wales Law Journal*, 37:2, 643–678.

(5) See Jillson, E., Federal Trade Commission, 'Aiming for truth, fairness, and equity in your company's use of AI' (19th April, 2021), available at https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai (warning companies against selling or using demonstrably biased AI systems pursuant to the FTC's authority to prohibit unfair and deceptive practices).

(6) National Artificial Intelligence Initiative Act of 2020, H.R. Res. 6395, 116th Cong. §§ 5001 et seq. (2020).

(7) *Ibid*. at § 5103(d)(2)(D).

(8) *Ibid*. at § 5301.

(9) *Ibid*.

(10) Anti-Money Laundering Act of 2020, H.R. Res. 6395, 116th Cong. §§ 6003 et seq. (2020).

(11) Board of Governors of the Federal Reserve System, Bureau of Consumer Financial Protection, Federal Deposit Insurance Corporation, National Credit Union Administration, and Office of the Comptroller of the Currency 'Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning', 86 FR 16837 (31st March, 2021), available at https://www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence.

(12) *Ibid*.

(13) *Ibid*.

(14) Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM 206 final (4th April, 2021), available at https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence.

(15) See Bank of England, Fintech AI Public-Private Forum (26th November, 2020), available at https://www.bankofengland.co.uk/events/2020/october/fintech-ai-public-private-forum.

(16) Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector, available at https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf (accessed 13th June, 2022).

(17) *Ibid*.

(18) *Ibid*.

(19) Office of the Comptroller of the Currency (August 2021), 'Model Risk Management', in 'Comptroller's Handbook', Version 1.0, available at, https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/model-risk-management/index-model-risk-management.html.

(20) Brainard, L., Governor, Board of Governors of the Federal Reserve System (13th November, 2018), 'Address at the Fintech and the New Financial Landscape Conference: What are We Learning about Artificial Intelligence in Financial Services?', available at https://www.federalreserve.gov/newsevents/speech/brainard20181113a.htm.

(21) Ananny, M. & Crawford, K. (2016), 'Seeing Without Knowing: Limitations of the Transparency Ideal and its Application to Algorithmic Accountability', *New Media & Society*, DOI:10.1177/1461444816676645.
(22) The United States Department of Justice, 'Human trafficking is a crime that involves exploiting a person for labor, services, or commercial sex'. 22U.S.C. § 7102(9), available at https://www.govinfo.gov/content/pkg/USCODE-2020-title22/pdf/USCODE-2020-title22-chap78-sec7102.pdf.
(23) US Dept. of Treasury (2020), 'National Strategy for Combating Terrorist and Other Illicit Financing', available at https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf.
(24) FinCEN (15th October, 2020), *Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity*, FIN-2020-A008, available at https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2020-a008.
(25) H.R. Res. 6395, 116th Cong. § 6505 (2020), available at https://www.congress.gov/bill/116th-congress/house-bill/6395.
(26) OCC, Bank Secrecy Act/Anti-Money Laundering: Interagency Statement on the Issuance of the Anti-Money Laundering/Countering the Financing of Terrorism National Priorities (30th June, 2021), 'Bulletin 2021-29', available at https://www.occ.gov/news-issuances/bulletins/2021/bulletin-2021-29.html.
(27) ACAMS and Leichtenstein Initiative (2020) 'Fighting Modern Slavery and Human Trafficking', Finance Against Slavery & Trafficking, Online Training Certificate Reading Material, at 28–35, available at https://www.acams.org/en/training/certificates/fighting-modern-slavery-and-human-trafficking#overview-ce6f8a18, (accessed 2nd June, 2022).
(28) FinCEN (15th October, 2020), 'Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity', FIN-2020-A008, available at https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf.
(29) Office to Monitor and Combat Trafficking in Persons, US Dept. of State (June, 2021), *The Role of the Financial Sector: Promising Practices in the Eradication of Trafficking in Persons*, available at https://www.state.gov/wp-content/uploads/2021/06/The-Role-of-the-Financial-Sector-Promising-Practices-in-the-Eradication-of-Trafficking-in-Persons_LOW.pdf.
(30) See Herrmann, T. (December, 2021) Research & Development Team, National Ugly Mugs, Financial Discrimination of Sex Workers in the UK, 'A report from National Ugly Mugs', available at https://nationaluglymugs.org/wp-content/uploads/2022/01/BDSW_final.pdf (report based on a survey of consumers engaged in lawful sex work who experienced account closure, money seizure, or declined accounts, loans and overdrafts on the basis of occupation); see also Watson, S. & D'Adamo, K. (2021) Center for LGBTQ Economic Advancement & Research, 'Shut Down & Shut Out: Access to Financial Services and Online Payments for Sex Workers in the U.S'. Available at https://lgbtq-economics.org/wp-content/uploads/2021/06/Shut-Down-Shut-Out.pdf.
(31) See US Dept. of State, Off. to Monitor and Combat Trafficking in Persons (2021), 'The Role of the Financial Sector: Promising Practices in the Eradication of Trafficking in Persons 2', available at https://www.state.gov/the-role-of-the-financial-sector-promising-practices-in-the-eradication-of-trafficking-in-persons/ ('Survivors of human trafficking often discover that human traffickers have taken control of their financial identity or banking products and limited or prevented their access to the financial system, spoiling their credit record and hindering their financial reintegration'); see also, Byrne, S. et al. (27th January, 2022), Alliance 8.7, 'Financial Recovery and Reintegration of Survivors of Human Trafficking' available at https://delta87.org/2022/01/can-new-us-law-help-increase-financial-recovery-reintegration-survivors-human-trafficking/ ('A trafficker may require or coerce victims to open, close, or mismanage bank accounts and credit cards, or engage in other activity that leads to "bad credit". They may also fraudulently use or "hijack" victims' identification to access credit and commit financial crimes for many years after the survivor has exited the trafficking experience, thereby extending the period of exploitation').