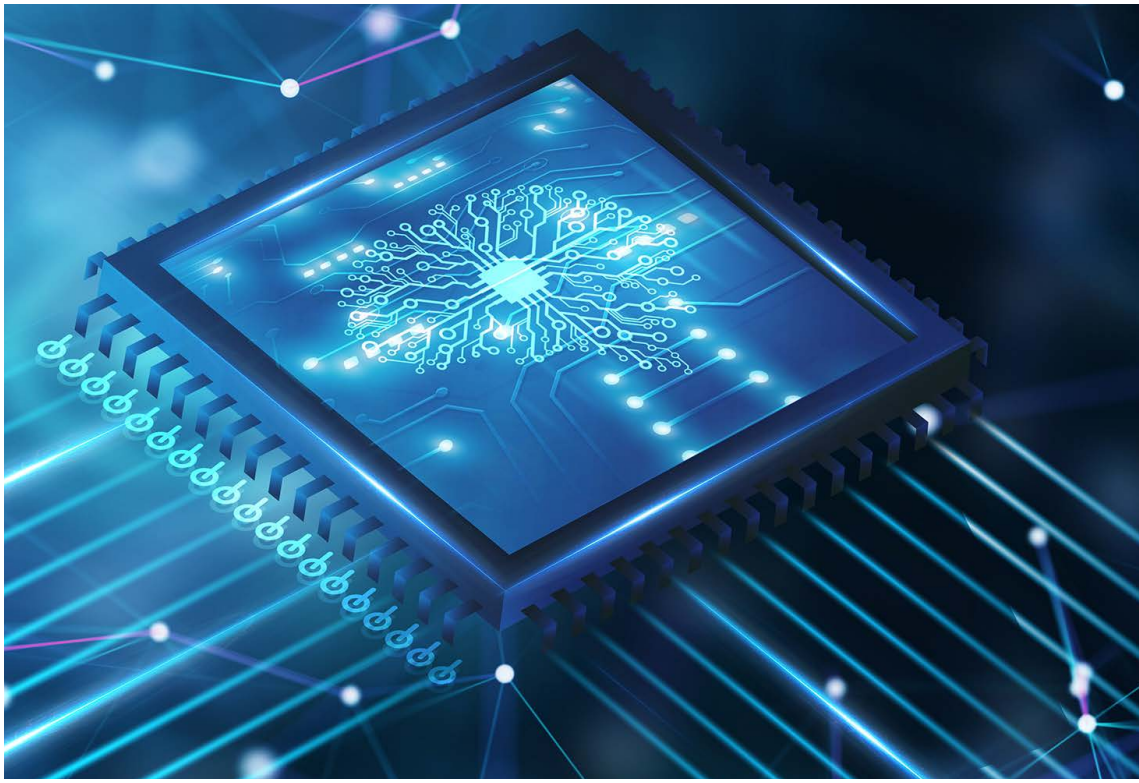
Artificial intelligence in banking

Risks and benefits

Risk Universe
by RiskBusiness



WHAT IS AI?

There is no official definition for artificial intelligence (AI), but it is often referred to as something along the lines of "the science of making computers do things that require intelligence when done by humans." When we talk about AI, we often talk about machine learning too. Machine learning (ML) is a subset of AI and refers to the development of AI systems that are able to perform tasks as a result of a 'learning' process that relies on data. An example of this is targeted online advertising; when you have been researching a product online and as a result, are 'followed' by adverts for this product on every website you visit.

In the context of retail banking, these "intelligent" automated activities might include algorithms used to assess an individual's credit quality, price their insurance or recommend products and services. AI is also used in middle-office processes such as model risk management and stress testing, and also in trading and investment such as algorithmic trading and portfolio management. Many RegTech solutions such as fraud detection systems, AML compliance and regulatory change programs also rely on the use of AI.

CURRENT AI REGULATION

AI regulation is still very much in the development phase, despite use of the technology being widespread. This is because of the fast-moving nature of AI and ML; the technology is evolving all the time, leaving governments and regulators to play catch up. However, several jurisdictions are making moves to address gaps in regulation for the use of AI in the financial sector, as discussed below.

BANK OF ENGLAND DISCUSSION PAPER

The Bank of England launched a discussion paper in October 2022 with the aim of determining whether existing regulation and guidance is sufficient in addressing the

associated risks of using AI and to hopefully identify any areas that could be developed to help mitigate AI-specific risks.

Questions in the discussion paper are split into three categories:

- **Supervisory authorities objectives and remits**
  Questions in this category attempt to create a scope of what actually constitutes as AI and should therefore be subject to regulation.
- **Benefits and risks of AI**
  These questions aim to identify the potential risks and benefits of AI in order for regulators to prioritise these areas.
- **Regulation**
  These questions are designed to critique the current regulatory landscape to see if it could be made more fit-for-purpose for AI-specific activities, including whether current regulation may conversely create a barrier for the safe and responsible adoption of AI in finance.

DEFINING AI: EXISTING FRAMEWORKS

One of the critical challenges to regulating AI is first defining it. The Bank of England discussion paper proposes two approaches to defining AI: a precise, legal definition; or a broader spectrum of varying analytical techniques.

There are several existing frameworks that provide a broader definition of AI and its applications, including the OECD's (Organization for Economic Cooperation and Development) Framework for the Classification of AI Systems, which was published in February 2022. The framework is designed to provide a tool for the evaluation of AI systems in order to build policies around its use and to help regulators, legislators and others characterise AI systems deployed in specific contexts.

The framework is not specific to any one industry or sector but provides a generic basis by which to assess risks that are typically associated with AI, such as bias, explainability and robustness: "It facilitates nuanced and precise policy debate," says the OECD. "The framework can also help develop policies and regulations, since AI system characteristics influence the technical and procedural measures they need for implementation."

THE EU AI ACT

The EU is the first major regulator to propose an actual law on AI. The law splits the use of AI into three distinct risk categories: "Applications and systems that create an unacceptable risk, such as government-run social scoring of the type used in China, are banned." High-risk applications, "such as a CV-scanning tool that ranks job applicants, are subject to specific legal requirements." The third category is applications "not explicitly banned or listed as high-risk", which are largely left unregulated.

Like the GDPR (General Data Protection Regulation) before it, the EU AI Act is likely to become a global standard and so firms in all jurisdictions should pay close attention to its progress. Proposed fines for non-compliance with the final law will be similar in size to those issued in relation to GDPR non-compliance: up to a maximum of 6% of the firm's global annual turnover. The law will impact not just providers of AI systems, but also any organisation that makes use of them.

The EU is the first major regulator to propose an actual law on AI

> **"The United Nations' Office on Drugs and Crime estimates that less than 1% of financial crime is caught"**

BENEFITS OF AI IN BANKING

AI is already part of our daily lives and used by systems we interact with on a daily basis. The benefits of AI in banking include the ability for banks to make quicker but better-informed investments, detect suspicious activity such as credit card fraud or money laundering, reduce human error and improve customer experiences by boosting efficiency. Because the volume of data collected and processed by banks is so vast, it cannot be managed by manual processes and human decision-making alone. Even the financial regulators (who ironically will also be responsible for regulating the use of AI in banking at some point) must deploy artificial intelligence and machine learning themselves, in order to monitor the firms under their jurisdiction.

The Russian invasion of Ukraine provides a working example of how AI could be better deployed across agencies. "Financial institutions are required to screen accounts and transactions to identify transactions by sanctioned entities," writes Jo Ann Barefoot, CEO of the Alliance for Innovative Regulation, in an article for The Brookings Institution (a non-profit public policy organisation based in Washington, DC). "What if they and law enforcement agencies like the Financial Crimes Enforcement Network (FinCEN) had AI-powered analytics to pull and pool data from across the spectrum of global transactions and find the patterns revealing activity by sanctioned parties? Unfortunately, most financial institutions and government agencies do not have these tools in hand today."

Barefoot argues another example can be drawn from the increase in human trafficking as a result of the conflict in Ukraine. "Banks are required by law to maintain anti-money laundering (AML) systems to detect and report money movement that may indicate human trafficking and other crimes, but these systems are mostly analog and notoriously ineffective," she says. "The United Nations' Office on Drugs and Crime estimates that less than 1% of financial crime is caught. AI-powered compliance systems would have a far better chance of flagging the criminal rings targeting Ukraine. If such systems had been in effect in recent years, moreover, the human trafficking trade might not be flourishing."

WHAT ARE THE RISKS?

Just as the use of AI accelerates a bank's ability to onboard clients, or place trades,

or detect money laundering activity, it also accelerates the potential risk impacts. "Compared to human decision-making, the nature and the increasing use of AIDA [artificial intelligence and data analytics] may heighten the risks of systematic misuse," says the Monetary Authority of Singapore in its guidance document entitled *Principles to Promote FEAT (Fairness, Ethics, Accountability and Transparency) in the Use of AI and Data Analytics in Singapore's Financial Sector*. "This may result in impacts which are more widespread, perpetuated at greater speed."

CUSTOMER OUTCOMES

There are several frameworks that have been published which try to identify these risks and provide a practical model for managing them. One of the key issues referred to in the majority of the documents reviewed for this report – and the key focus of the MAS guidance referenced above – is maintaining an ethical and transparent way of working that prioritises consumer outcomes at all times, ensuring that commercial gain doesn't come at the expense of the individual and subsequently the bank's reputation. Regardless of whether or not specific AI laws or regulation are currently in place, firms still need to ensure that their use of AI isn't impacting compliance in other areas of regulation.

For example, in the UK, the Consumer Duty currently being imposed by the FCA places increased emphasis on firms being able to demonstrate they meet their obligation to always act in the interest of their customers. Not having a full understanding of the risks associated with AI and ML and not being truly aware of how it is embedded within daily operations and how it impacts consumers, could easily put firms at risk of breaching these obligations.

"One of the key problems here is knowledge - or rather, a lack thereof," says RiskBusiness CEO, Mike Finlay. "Accountability is obviously important when it comes to the use of automated, data-driven systems. But if you are relying solely on the competence of others, saying you 'approve' the use of AI in decision-making processes doesn't really mean anything. The Board needs regular updates on the use of AI so they can be aware of the potential consequences of any AI-driven decisions – both good and bad. And firms should also be thinking seriously about who is sitting on the Board; where are the experts in AI and are Board members asking the right questions?"

According to a survey of C-suite executives carried out by global analytics firms FICO and Corinium in 2021, 65% of respondents could not explain how their AI models make decisions for their firm. The study surveyed 100 C-level executives from global enterprises with revenues in excess of US$100m, all with job titles such as Chief Data Officer, Chief Analytics Officer, Chief Data and Analytics Officer and Chief AI Officer. Entitled, *The True Extent of the AI Ethics Problem*, it looked at how organisations are prioritising the ethical implications of AI. "The thorny ethical implications of the arrival of AI are rich and varied," says the report. "While most enterprises adopting AI technologies may not be faced with life or death choices, all of them are at risk of reputational damage. "

Perhaps unsurprisingly, it is the risk and compliance teams who appear to have the

Where are the experts in AI and are Board members asking the right questions?

A Microsoft chatbot called Tay spent a day learning from Twitter and began spouting antisemitic messages

most awareness of ethical issues surrounding AI so far. According to the survey, "more than 80% of staff in these roles have a complete or partial understanding of the problem. They also rated awareness in IT and data and analytics teams highly, at well over 70%."

ALGORITHMIC BIAS

The risks long-associated with human bias in banking-based processes such as mortgage approval have now largely shifted over to algorithmic bias. Algorithmic bias refers to the way in which algorithms are programmed to make decisions which create outcomes that may be deemed unfair, such as favouring one group of people over another, in a way that is not the intended purpose of the algorithm.

Back in 2017, an article written by Stephen Buranyi for *The Guardian's* Inequality Project looked at how AI is learning some of humanity's worst habits and reproducing them on a colossal scale, sometimes undetected for years. "Programs developed by companies at the forefront of AI research have resulted in a string of errors that look uncannily like the darker biases of humanity," writes Buryani. "A Google image recognition program labelled the faces of several black people as gorillas; a LinkedIn advertising program showed a preference for male names in searches, and a Microsoft chatbot called Tay spent a day learning from Twitter and began spouting antisemitic messages… When the data we feed the machines reflects the history of our own unequal society, we are, in effect, asking the program to learn our own biases."

Wells Fargo is currently facing a class-action lawsuit over alleged bias in the algorithms it deploys to approve mortgages. "Wells Fargo's algorithm labels certain neighbourhoods that are predominantly black as neighbourhoods ineligible for rapid loan processing, a service provided to similarly situated white applicants," says the lawsuit. "As a result, Wells Fargo loan personnel have told African American loan applicants who live in predominantly black neighbourhoods that they would not receive the same rapid application process as their white counterparts."

The lawsuit also claims that black applicants were more likely to give up during the application process because of additional barriers they experienced compared to white applicants. According to

the lawsuit, a white applicant looking to remortgage, who earned between US$0 and US$63,000 per year was "more likely to have their home loan financing application approved by Wells Fargo than a black applicant seeking to refinance their home loan, who earned between US$120,000 and US$168,000 per year. As a result of Wells Fargo's barrage of pretextual actions aimed at deterring black applicants, more than one-quarter of all black homeowners who began an application to finance their home loan through Wells Fargo did not finish their application."

An investigation carried out by *Bloomberg* found Wells Fargo only approved 47% of loan applications by black borrowers in 2020, compared to 72% of white customers. Other lenders approved a combined 71% of their black customers' applications.

DATA PRIVACY/SAFETY

There are two sides to the data privacy discussion when it comes to AI. One argument is that due to the vast swathes of data used in AI, some of it will undoubtedly be sensitive personal information which may not always be completely anonymised, or could potentially be de-anonymised further down the line and used to identify individuals. Plus, there is the consent issue: do consumers really understand how their data will be used? "Companies need to make a significant effort at clarity and transparency regarding more complex uses and insights from AI that users may not readily understand, like psychological or behavioural insights that can be determined from the data analysis," say consent management experts, Usercentrics. "Since AI needs a great deal of data, it is likely this data would come from a number of sources. This would mean a significant requirement for strong data protection and security practices when the data is collected, shared, and stored. If AI processing is done by a third party, they and the data controller for whom they're working must also be careful to comply with regulatory requirements for the safeguarding and use of data for AI analysis."

The other side of the argument is that AI's true potential to improve efficiency, accessibility and usability for the masses cannot ever be fully realised if it is overregulated. "Probably the greatest challenge facing the AI industry is the need to reconcile AI's need for large amounts of structured or standardised data with the human right to privacy," says London's Royal Institute of International Affairs. "AI's 'hunger' for large data sets is in direct tension with current privacy legislation and culture. Current law in the UK and Europe limits both the potential for sharing data sets and the scope of automated decision-making. These restrictions are limiting the capacity of AI."

This is not the case in all jurisdictions though. For example, in China, where laws around privacy and surveillance are far less clear, companies specialising in the development of AI software have been able to capitalise on access to reams of publicly available data.

> **"AI's 'hunger' for large data sets is in direct tension with current privacy legislation and culture"**

OUTSOURCING: ADDING COMPLEXITY

Outsourcing in the context of AI provides an added complication to an already

Only 25% of Gen Z consumers use a large, traditional bank for their current account

complex journey for consumer data. Not only do you have to ensure you are building third-parties into your risk assessments, with particular focus on data security; there are also risks surrounding how that data is handled and processed by a third party. "If two people with very similar personal information, coming from more than one system, get merged into one record erroneously, not only could one person receive offers they're not interested in, as a mild consequence, it could be a legal violation, as the person receiving the offers did not opt in," says Usercentrics. "It could have been the other person who agreed to data collection and communications, but who, from the standpoint of the harmonised data, has ceased to exist."

KEEPING UP

For traditional financial institutions, the use of AI and ML is not only desirable but is also necessary in order to compete with industry disruptors. According to another FICO survey, the percentage of Gen Z, Millennial, and Gen X consumers in the US who use a digital bank as their main account provider has more than doubled since 2020, and only 25% of Gen Z consumers use a large, traditional bank for their current account. If traditional banks want to survive, a better understanding and a more-impactful adoption of AI will be essential.

"As the regulation of this area is still in its infancy, it will fall to compliance and risk management teams to help navigate the risks of this new landscape," says RiskBusiness' Mike Finlay, "and research suggests they are already leading the way. Firms have an opportunity to be proactive and instil their own principles of best practice before they become regulatory obligations – lightening the load further down the line."

About Risk Universe

Risk Universe by RiskBusiness provides in-depth analysis, reviews and research on areas of interest within the broader governance, risk, audit and compliance landscape, designed to provide proactive, 360° intelligence for informed decision making across the enterprise.

About RiskBusiness

RiskBusiness is an international governance, risk, audit and compliance (GRAC) solution provider, delivering risk content, risk intelligence, risk tools and risk advisory services to its clients. It is an association of like-minded industry professionals, who have the aim of furthering the risk management discipline to enable better risk-reward decision making.

Risk management is an evolving discipline, which has developed in close partnership with the industry. RiskBusiness has, both as individuals and collectively, a depth of established relationships with leading players and regulators in the operational risk field. We are also active participants in industry working groups and contribute thought leadership through publications and education.

RiskBusiness was founded in 2003 and today has principal locations in Birmingham, London, Buenos Aries, Amsterdam, Hong Kong, New York, Singapore, Toronto, and Zurich. To learn more, visit **www.riskbusiness.com**

Contacts

Carrie Cook, Editor:
carrie.cook@riskbusiness.com

General enquiries:
info@riskbusiness.com

Risk Universe
by RiskBusiness

www.riskbusiness.com