ARTIFICIAL INTELLIGENCE IN FINANCIAL SERVICES

CHARLES KERRIGAN | Partner, CMS
ANTONIA BAIN | Lawyer, CMS

ABSTRACT

The integration of artificial intelligence (AI) systems within the financial services industry has the potential to transform business operations, improve customer relations, and enhance regulatory compliance efforts. However, its adoption is not without risk; the integration of AI raises significant ethical concerns and threatens market integrity, data privacy, consumer protection, and other modern tenets of law. While these concerns are not necessarily new to the financial services industry, they do present barriers to the incorporation of AI technology. This article explores both the benefits and risks associated with AI in the context of financial services, discussing the relevant policy considerations and current regulatory landscape. It synthesizes current research and industry invites to provide an overview of the opportunities and challenges associated with the use of AI within financial services while addressing the lack of certainty currently observed in formulating an approach for broader incorporation. In doing so, this article offers valuable insights for financial professionals and researchers in navigating the rapidly evolving landscape of AI-driven financial services.

1. WHAT IS ARTIFICIAL INTELLIGENCE?

Artificial intelligence (AI), for present purposes, can be defined as algorithmic and/or machine-based systems with the capabilities to carry out functions that would otherwise necessitate human thinking or intervention.[1] Essentially, it represents the combination of machine-learning and robust datasets to enable software to show learning, adaptability, and perform cognitive tasks (including problem-solving and decision-making functions, among other things).[2]

In practice, AI can be considered in specialized sub-categories, with each allowing for different operational outcomes and purposes. For example, predictive AI adopts a statistical analysis of past patterns and events in order to predict future outcomes. Generative AI (GenAI) considers large quantities of inputted data to produce new outputs, such as recommendations or answers to inputted questions.

The increasing speed of adoption of new AI systems provides opportunities for efficiency in terms of time, cost, and outcomes; however, its adoption is not without risk. While many of these risks are not new, there is a degree of uncertainty in the application of AI across various industries; as such, its rapid and widespread integration may attach new challenges for regulators which, in turn, may create barriers to the effective implementation of the technology. The following shall consider the adoption of AI across the financial services sector, focusing on its use-cases and the regulatory landscape.

2. HOW IS AI RELEVANT TO FINANCIAL SERVICES?

The financial services sector is subject to industry-specific regulation, leading to some natural reluctance among industry participants in adopting innovative technologies; as such, the initial uptake of AI was cautious. However, AI systems perform well in tasks that are core to the activities of financial

[1] https://tinyurl.com/2bk6s27n
[2] https://tinyurl.com/2e53h75x

AI in financial services

AI has and will continue to observe increasing capital investments and annual growth:

- A recent survey shows that 42% of 56 U.S. financial services executives plan on increasing AI investments by at least 50%.
- AI in financial services has a predicted annual growth of 20-34% in the Middle East.
- According to KPMG, 84% of UK financial services business leaders say that AI is at least moderately to fully functional within their organization.[3]

Such growth is at least partly attributable to the continuing development of the technology underpinning AI, which continues to improve upon AI's understanding and generative activities. Public Alpha chatbot exemplifies the increasing sophistication and power behind AI. To expand, the model is underpinned by approximately 1.2 billion parameters, all of which support the chatbot to engage in its processing functions, generate responses, and even grasp nuance. These functions and the increasing parameters are leading to outputs that are "indistinguishable from those a human might produce."

institutions. A recent study by U.K. Finance showed that 91% of financial institutions have now deployed some level of predictive AI in fraud detection and back-office functions, with recorded benefits. To this end, financial services firms continue to embrace different forms of AI to optimize their operations and enhance customer services. For example, AI is now widely used to leverage data, automate tasks, and deliver personalized services to clients, with common applications including:

- the deployment of chatbots and robo-advisors
- fraud and money laundering detection
- know your customer (KYC) checks
- creditworthiness assessments for loans and mortgages (with examples of banks in the U.S. adopting GenAI solutions to support with small business lending)
- automation of insights from earnings transcripts and analysis of data in investment management.

Broadly speaking, such applications have the potential to significantly improve the operational outcomes for both businesses and consumers, while concurrently limiting various risks commonly associated with the financial services industry. In addition, they may serve to support the regulatory compliance efforts of financial institutions through promoting operational resilience and facilitating firms' consumer duty.

In addition to the aforementioned operational enhancements, AI is transforming the business models of financial institutions. Service providers now offer "AI as a service" (AIaaS) to financial services firms; this involves a cloud-based AI outsourcing solution that enables organizations to adopt and test AI systems without incurring significant capital expenditure and without assuming many of the risks. In turn, financial institutions are integrating AI and machine-learning solutions into their supply chain, marking a shift from traditional business-to-business (B2B) or business-to-consumer (B2C) models to more complex structures like B2B2C or B2B2B. This evolution involves financial institutions acting as intermediaries, procuring AI solutions from third parties and bundling them into comprehensive product packages for clients. This shift not only reflects the industry's commitment to technological advancement but also underscores the importance of collaborative ecosystems in the modern financial landscape.

The below sets out two key use-cases of AIaaS, demonstrating the practical efficiencies to be derived from AI integration in FS.

3. RISKS AND ETHICS

The underlying risks and ethics of AI systems have been central to discussions on their application in virtually all industries, including in financial services. The Bank of England (BoE) recently reported that the risks presented by AI in the context of financial services can be considered under three categories, namely: (i) data, (ii) models, and (iii) governance. For present purposes, these risks will be considered in terms of those that are already seen within financial services and those that may be introduced with the adoption of AI.

3.1 Traditional finance

As an innovative technology, AI presents new challenges for regulators and industry participants; however, it also adds uncertainty and may exaggerate traditional industry risks. For example, the financial services industry is inherently subject to "bad actor" risks; these include instances of

[3] https://tinyurl.com/bdftwd5x

AI and fraud detection

AI integration has the potential to improve operational efficiency and practical outcomes as it may detect instances of fraud before they are carried through. To the extent that card and digital wallet payments are projected to account for 86% of payments by 2026,[4] and insofar as fraud cases continue to rise, the application of AI in fraud detection will likely prove of significant utility.

To expand, the incidence of fraud in the financial services industry continues to increase in prevalence. The Identity Theft Recourse Centre found a 78% increase in data compromises between 2022 and 2023, while Deloitte found a 90% increase in P2P payment fraud losses between 2021-2022. In other words, card fraud losses are in excess of U.S.$33 billion per year.

Various financial services firms have incorporated AI fraud detection software to varying degrees. Most of these systems rely on "synthetic minority oversampling techniques" (SMOTE), whereby synthetic examples of fraud cases (i.e., the minority of cases) are used to balance the dataset. Through focusing solely on fraud cases, the model addresses concerns observed in traditional detection mechanisms, namely, where cases of fraud were not identified. However, this model proves to be overly responsive in its detection insofar as it is predicated on information relating to fraud cases; in practice, this has led to too many cases of potential fraud being identified with the model producing a number of false positives. Such false positives inhibit the efficiency of transactions and have resulted in annual losses of U.S.$443 billion to merchants.

In response to the increasing incidence of fraud and faults identified in the current AI detection methods, Mastercard has released Digital Intelligence Pro. This is an in-house-built AI model that has been developed to detect fraud while minimizing the incidence of false positives and ensuring market efficiency. It utilizes a "recurrent neural network" (RNN); having received the data from approximately 125 billion transactions flowing through Mastercard, the AI is trained to detect fraud within a multitude of transaction types (rather than solely focusing on instances of fraud). In doing so, it appears to reduce the bias that has previously led to shortcomings in AI analysis, with evidence suggesting that (at its current state of development) the Digital Intelligence Pro has the capacity to improve fraud detection rates by 20%.

market manipulation, insider threats, and cybersecurity threats, among others. Introducing AI to bad actors may serve to heighten such risks; in our cybersecurity example, hackers may leverage the machine learning presented by AI to enhance the efficiency and sophistication of their attacks. Further, it can permit instances of market manipulation and insider threats insofar as datasets may be tampered with to produce outcomes benefitting specific persons.

Similarly, data and consumer protection risks persist. AI systems may interact with and process customer data to produce outcomes that adversely affect such customers; such outcomes include, but are not limited to data leaks, discrimination, and unfair treatment of consumers.

However, the aforementioned risks all existed in some form prior to the integration of AI. Further, such risks will continue to exist insofar as they are a product of the industry's substantive operations and outcomes. In turn, existing regulation (as applicable to traditional financial services) may prove sufficient in addressing such risks, irrespective of the added uncertainty presented by AI.

This is not to say that AI does not present its own challenges;[5] rather, it highlights that the risks AI simply exaggerates may be sufficiently addressed through existing legal provisions.[6] The E.U. AI Act purports to address some of these concerns in more detail, focusing on the mitigation of some of these risks; as discussed further in Section 6, the Act shall apply as overarching regulation, covering both general and industry-specific risks associated with AI systems.

3.2 The risks associated with AI

As a developing and innovative technology, AI adoption presents unique ethical considerations and risks. Relevant stakeholders have formulated various standards for ethical AI use, including transparency and accountability, along with

[4] https://tinyurl.com/ymb4z3bu
[5] See Section 3.2.
[6] See Section 5.

other considerations;[7] however, to date, there has been little in the form of directly applicable legal standards. Accordingly, where existing legal regimes prove insufficient, such risks will persist and may create barriers to the effective implementation of AI in practice. The below will set out some of the perceived risks associated with the adoption of AI specifically. This is a non-exhaustive list and remains subject to change as the technology develops.

3.2.1 LEGAL UNCERTAINTY AND ALLOCATION OF LIABILITY

First and foremost, there is a lack of certainty as to the bounds of control and the legal categorization of AI; this issue has been observed even in jurisdictions where we have seen text of directly applicable AI regulation. Naturally, this creates uncertainty as to the proper allocation of liability which, in turn, creates barriers in the adoption of the technology.

While it is apparent that AI has not yet been attributed separate legal personality, there remains uncertainty in practice as to the appropriate attribution of responsibility. This is largely due to the complexities associated with the technology; AI is predicated on machine learning (i.e., it removes the need for human intervention), which implies that the outcomes are, in the most direct sense, not reliant on the actions or omissions of a person. While it could be argued that human intervention has been necessary in the development of the technology, the issue remains with whether the provider or developer can be deemed to owe a duty or obligation towards the claimant. In some instances, the answer may be clear (particularly where contractual arrangements are involved); however, in others, and particularly as the technology advances, the acts or omissions may be deemed too remote for the provider or developer to be held liable.

Further, there is often a lack of transparency and opacity in the parties responsible for the underlying AI; thus, actually determining the identities of the parties potentially responsible for the harm may prove fruitless in itself.

Without any statutory or contractual rights, those who have suffered harm due to interactions with AI have limited recourse. They may seek redress through traditional routes, such as tort; however, without clearly defined obligations and allocation of responsibility, the aforementioned complexities will create barriers to proving a viable action. In this sense, practical issues have played a part in preventing legal certainty. Any claims for damages caused by an interaction with AI systems would likely prove prohibitively expensive and time-consuming, with the likelihood of success proving too uncertain to justify such costs. Accordingly, the courts have had limited opportunities to clarify the legal position and such uncertainty persists.

This lack of certainty creates concerns for organizations in incorporating AI systems, with liability concerns being found to be the most relevant external obstacle in the corporate adoption of AI.[8] To expand, organizations face the risk of assuming liability for claims brought due to harms caused by AI systems, which may deter them from incorporating the technology. Further, both consumers and businesses bear the risk of uncompensated harm; naturally, this will undermine trust and confidence, acting act as a barrier to incorporation. From this, it is clear that a greater degree of legal certainty and improved transparency requirements will be necessary in ensuring efficient and effective practical outcomes.

Regulatory technology and supervisory technology

Regulatory technology (regtech) involves the use of technology (including the aforementioned cloud-based integrations) that purport to improve the efficiency of **financial services institutions** in managing their regulatory risk and complying with their regulatory obligations. For example, such technology can support financial services firms with regulatory and audit reporting, in producing business impact assessments and continuity plans, as well as in their AML processes.

Supervisory technology (suptech) is adopted by **supervisory authorities** in managing their regulatory compliance efforts. In this context, authorities can use suptech to support their operational and administrative efforts, such as data analysis in transaction reports to regulators as are required to be provided by regulated firms. It can also facilitate in regulatory reporting (through standardization and automated validation), compliance and market monitoring, and in the determination of risk across various industries.

[7] https://tinyurl.com/4u4wtsmd; https://tinyurl.com/yt7tjwn3; https://tinyurl.com/6cptdah

[8] EUR-Lex – 52022PC0496 – EN – EUR-Lex, Explanatory Memorandum, https://tinyurl.com/2s3pbp6x.

In traditional practice, the financial services industry has sought to resolve such issues through regulation. In the U.K., the financial services industry is subject to the Senior Managers Regime, industry principles (as discussed in Section 5), and various other forms of regulation. For example, the Listing Rules require companies to make certain disclosures and seek to maintain transparent, fair trading practices. While the introduction of AI systems may add opacity to the financial services industry, it is submitted that proper legislative intervention (similar to that proposed by the E.U. AI Act, as discussed in Section 6) may serve to mitigate the aforementioned confusion.

3.2.2 ROBUSTNESS AND SAFETY

(i) **The underlying dataset**

As noted, AI has the potential to bring significant operational efficiencies (such as fraud detection) and may support in financial services functions and outputs;[9] however, industry participants (including the BoE) have expressed concerns that such integration could implicate the soundness of firms that choose to adopt the services. In practice, AI systems may produce inaccurate outputs. This is not unique to AI, rather the risk exists due to faulty datasets; however, the involvement of AI means that the erroneous outputs could prove to be more widespread and persistent than if they had occurred due to human error. In practice, these faulty outputs could lead to significant and even systemic harms; for example, consistently inaccurate determinations of credit risk could lead to "inaccurate capital modelling".[10]

Further, many AI systems are programmed to be adaptable insofar as they are continuously learning from the inputted datasets; while this allows for flexibility in outputs, it exaggerates the risks of data and concept drifts (and, therefore, the risk of invalidating the data model). As identified by the BoE, if an AI system is found to be insufficiently transparent or too complex, then there is a high likelihood that prudential risks (including credit and operational risks, as well as systemic risks) will arise. Naturally, such risks threaten the integrity of financial services businesses and pose significant risks to consumers.

These risks may be mitigated by the Principles for Effective Risk Data Aggregation and Risk Reporting requirements (the BCBS), at least to some degree.[11] Essentially, the BCBS requires financial institutions to establish and implement robust governance and oversight mechanisms designed to ensure effective data aggregation and reporting.

Financial institutions are responsible for ensuring that any AIaaS providers they engage will comply with such requirements; this is required per financial regulation outsourcing rules insofar as financial institutions must implement various

Case study: oxyML LLC

One of the primary areas of inspection of the FCA – and other regulators in many other markets – is whether a given asset allocation at a managed fund is consistent with the stated goals and risk levels discussed in their offering documentation. This can be seen in CP 19/5 and tangentially in parts of the Investment Funds Prudential Regime (IFPR) and Internal Capital Adequacy and Risk Assessment (ICARA). Increasingly, firms are being asked to provide more data and analysis to support their level of risk taking and justify allocations to different assets. This is a challenge for many firms, which have deprioritized data services to back-office compliance and documentation relative to pre-trade allocation analytics. This continues to be a challenge as firms grapple with legacy software not designed for extensive external data reporting.

When properly implemented, AI provides an opportunity to significantly enhance back-office activities by feeding in proper data and setting appropriate constraints. Proper implementation is far from straightforward, as base natural language processing systems such as ChatGPT will report factually inaccurate information that at first glance appears correct.

oxyML's Voltsail system was able to circumvent these issues combining patented constrained optimization algorithms with heavily restrictive rules-based logic systems, resulting in verifiable, zero-trust automated documentation and compliance support. As a result, oxyML was able to ensure proper management and support of billions of dollars in assets at partner asset management institutions across the U.S. and the U.K.

[9] See Section 2.
[10] Bank of England, 2022, "Artificial intelligence and machine learning," at 3.17, https://tinyurl.com/47xds9dh
[11] BIS, 2013, "Principles for effective risk data aggregation and risk reporting," https://tinyurl.com/mvsfx7ej

procedures and oversight checks before and during any engagement with a third-party service provider.[12] In practice, this acts to ensure that recorded and inputted data is likely to be accurate and, therefore, risks attributed to data faults are somewhat mitigated; however, to the extent that this cannot be guaranteed, this remains a point of concern.

The E.U. AI Act also aims to address these concerns insofar as it creates a requirement for human oversight.[13] Briefly, AI systems will need to be developed in such a way that they can be "effectively overseen by natural persons"; in effect, this follows the policy aims of the BCBS insofar as such human oversight should reduce the risk of poor or inaccurate data.

(ii) **Market stability and integrity**

In principle, AI promises to promote and protect market integrity within financial services; the technology may be used to facilitate market surveillance (detecting instances of non-compliance) while concurrently allowing firms and regulators to assess and manage market risks. However, its adoption also poses a threat to such integrity. For example, bad actor risks could result in data breaches, misuse of assets, or widespread losses. Flash crashes caused by high-frequency trading algorithms (as facilitated through AI) may destabilize the financial markets and disrupt typical trading operations.

The concentration of the best AI systems within a small number of firms may threaten competition, lead to data monopolization, and create predatory, opaque pricing strategies. Naturally, this threatens the integrity of markets and creates significant risks for consumers. Additionally, any overreliance on AI systems and algorithms could amplify the manifestation of conventional systemic risks, particularly where such technology is concentrated; here, a system or technology crash could render the interconnected, interoperable markets the subject of significant losses.

Once again, these are not new risks; rather, they attach to the adoption of any technology. In the U.K., the Financial Conduct Authority (FCA) is tasked with "protect[ing] the integrity of the UK financial system";[14] as such, there is an existing infrastructure in place whereby such concerns can be overseen by a regulator. The E.U. AI Act also aims to address the manifestation of such risks (specifically systemic risks) through regulating specific AI models that have the greatest potential to attach systemic risks.[15]

4. POLICY: LESSONS TO BE LEARNT

4.1 Policy considerations in financial services

When considering risk management in the financial services industry, it seems prudent to reflect on the policy considerations that were developed in the aftermath of the 2007/2008 financial crisis. The crisis exposed a number of systemic risks and shortcomings within the financial services industry, with the lessons derived therefrom proving of general and continuous relevance to the industry. In practice, the legislature should bear such policy considerations in mind when regulating the integration of AI systems within financial services insofar as such integration presents similar risks to those observed prior to the crisis. Accordingly, it is submitted that the following policy considerations should be front-of-mind in the legislative process:

- **Transparency:** prior to the financial crisis, financial instruments were deemed too complex and opaque, thereby blurring the risks associated with the products. As noted, AI systems and structures are often complex and opaque, thereby limiting the ability of courts, regulators, and consumers to determine the risks attached to their use.
- **Data quality and bias:** the crisis emphasized that accurate, reliable, and unbiased data models are imperative to ensuring accurate products, pricing, and in estimating the degree of risk. Again, AI mimics these concerns insofar as inaccurate data poses a threat to consumers, as well as the integrity of businesses individually and the industry as a whole.
- **Sufficient oversight:** naturally, insufficient oversight of the financial services industry, its products, and compliance attempts contributed to the crisis. In considering the adoption of AI, it is submitted that sufficient regulatory oversight and understanding is required to mitigate the manifestation of the aforementioned risks; this, however, relies on sufficient transparency and proper data and models being in place.
- **Coordinated approach:** prior to the crisis, legislation and regulatory efforts were insufficiently cohesive among financial services sectors and across nations; insofar as the industry operates across borders, this lack of coordination exposed systemic risks and complicated response efforts. Again, AI is inherently cross-border;

[12] FCA Handbook, SYSC 8.1, available at: SYSC 8.1 General outsourcing requirements – FCA Handbook, https://tinyurl.com/25znv69p
[13] E.U. AI Act, Article 14
[14] About the FCA, https://tinyurl.com/5t42dnu9
[15] See Section 6.1.3; EU AI Act, Article 52.

to this end, ensuring some degree of consistency and coordination in regulatory efforts should act to mitigate such shortcomings.

- **Adaptive:** put simply, the financial crisis highlighted that financial regulation was insufficiently responsive to changes within the industry, with this leading to regulatory gaps and shortcomings. Insofar as AI and AI integration are evolving rapidly, it is submitted that any regulation must be able to adapt and respond to practical, industry developments in order to minimize regulatory pitfalls.

The U.K. government has affirmed that it wants to adopt a "pro-innovation approach" to AI regulation. In essence, they propose focusing regulatory efforts in a targeted, context-specific, and coherent fashion that permits for "safe" innovation.[17] The below summarizes the various policy statements and regulatory proposals as provided by the FCA and the U.K. government in respect of AI, highlighting how they align with and adopt the above suggestions.

Regulatory Genome Project

It is generally accepted that coordination in regulatory efforts should be considered in formulating financial services policy; however, given the volume, complexity, and divergence in existing financial services regulation, this is a time-consuming and difficult process. The Regulatory Genome Project (RGP),[16] as developed by Cambridge Judge Business School, aims to address this issue through its application of machine learning and AI.

To expand, RGP uses AI technology and machine learning to analyze and compare regulatory principles relating to financial services. Data relating to global financial services regulation is inputted into the AI system; after processing this data, the system is able to derive international principles and regulatory standards. This information is shared through a "common information structure", which allows regulators to quickly and "easily benchmark different regulatory frameworks," allowing them to prepare for innovative developments. In essence, this open information model simplifies the sharing of regulatory requirements and considerations among jurisdictions, thereby permitting for greater coordination, supporting effective supervision, and creating greater regulatory efficiencies.

4.2 U.K. government approach to AI policy

4.2.1 REGULATORY STRATEGY AND ATTITUDE

As noted, the U.K. government has committed to a "pro-innovation approach" in the regulation of AI and AI systems. In 2021, various government departments released the "National AI strategy" that set out the "ten-year plan" for ensuring the U.K.'s position as "a global AI superpower".[18] Essentially, the strategy inferred that the widespread implementation of AI systems was inevitable and, to ensure market competitiveness, the government needed to support this transition through well-crafted regulation. Recognizing the need for adaptable and robust rules, the proposal was underpinned by three overarching and strategic themes: (i) the need to promote investment and to plan for the long term, (ii) the need to capture the benefits of AI across all sectors and regions, and (iii) the need to ensure proper understanding and governance of AI systems.

Irrespective of this, the government recognized that implementing regulation should not be done until it has a proper and full understanding of the risks that such regulation seeks to address.[19] As such, in 2022, the Science, Innovation, and Technology Committee was tasked with launching an inquiry to explore AI's impact on society, economy, and regulation. The ongoing inquiry has received over 100 written submissions and 24 oral testimonies that will serve to guide and support the implementation of robust and appropriate AI governance frameworks.

4.2.2 REGULATION

In July 2022, the U.K. government proposed new regulations for AI use,[20] broadly aligning with the National Strategy. To expand, the proposal reaffirms that the government is "firmly pro-innovation" but recognizes that this needs to be balanced against a "pro-safety" approach in order to ensure the adoption of the technology and foster public trust. Notably, the proposal does not promote AI-specific laws or regulations;

[16] https://tinyurl.com/nrmaxeuf

[17] Letter from DSIT Secretary of State and the Economic Secretary to the Treasury and City Minister to the Financial Conduct Authority, https://tinyurl.com/3cxum2f4

[18] Guidance, "National AI strategy," updated December 18, 2022, https://tinyurl.com/ye22avk7

[19] As noted in Policy paper, "Establishing a pro-innovation approach to regulating AI," July 20, 2022, https://tinyurl.com/42hf8c86

[20] Ibid.

instead, it focuses on core principles that are to apply across all industries. These principles address the key risks attributed to AI systems, focusing on safety, transparency, fairness, accountability, and contestability. Irrespective of this, the specific implementation of such principles is subject to the discretion of the industry regulator (so, for the purposes of financial services, the FCA). In this sense, the proposed regulation appears to strike a balance between adaptability and robustness: it addresses the key risks attributable to AI generally while retaining sufficient flexibility to address industry specific concerns.

4.3 FCA comment on AI policy

The FCA acts to regulate and supervise the conduct of financial services firms within the U.K. In doing so, it determines appropriate rules and guidance applicable to financial services businesses and the industry more generally; accordingly, the FCA will be the body responsible for the specific implementation of the proposed principles governing AI in respect of financial services, as discussed above.

Together with the BoE and Prudential Regulation Authority (PRA) (collectively the "supervisory authority"), the FCA published DP5/22;[21] this report considered the specific application of AI regulation within the context of financial services, calling on industry participants to respond on issues including the degree and type of regulation. The report identified key risks relating to the integration of AI within financial services, including, but not limited to those of consumer protection risks and data concerns.

Once received, the industry responses and feedback were summarized in FS2/23.[22] Notably, many respondents were not in favor of sector-specific definition for AI given concerns of rapid technological advancements and regulatory arbitrage. Some respondents suggested AI-specific rules were unnecessary altogether. Further, it was suggested that greater national and international coordination was required to mitigate industry fragmentation. Broadly, these considerations align with the proposed policy considerations set out above.

Although the regulators continue to formulate regulatory standards, it can be concluded that financial services institutions should prepare for incoming AI regulations and look to align themselves with the guiding principles.

5. INDIRECT REGULATION

In some instances, the application of AI in financial services will not generate any novel risks or regulatory concerns; here, such risks can be addressed through legislation and regulatory provisions that would otherwise apply to the financial services industry and institutions. The following will demonstrate how the application of AI in financial services can effectively fall within existing regulations.

5.1 Consumer protection

As noted, AI can be utilized to identify consumers by virtue of specified characteristics; in doing so, firms can tailor their products and services to better support the consumer and their specific needs. For example, this application permits for the identification of vulnerable persons who may need additional support or be more susceptible to malicious activity. However, through such identification, consumers are at a heightened risk of exploitation, bias, and discrimination. Such technology may be used in respect of adjustable-rate mortgages (ARM); the application of such AI systems in ARM-monitoring puts consumers are risk of predatory lending practices and unfair treatment, which could serve to exacerbate inequalities or financial vulnerabilities. Such risks may manifest due to insufficient datasets or the programming and personalization of the technology.

While many firms have voluntarily implemented policies and procedures to address such concerns,[23] they will likely be subject to the FCA's Principles for Business ("the Principles") and,[24] when implemented, its policy of "A New Consumer Duty" ("the Duty").[25]

- The Principles are fundamental obligations placed on firms to protect customers and, in particular, retail customers. For example, firms are under an obligation to pay due regard to customers interest and treat them fairly, and they must act to deliver good outcome for retail customers. More generally, the Principles serve to heighten protections (particularly for vulnerable customers) and mitigate the risk of discrimination. While not specific to AI, the Principles place a general duty on regulated firms operating within the financial services industry. Further, such Principles will also apply to AIaaS when the third-party service provider interacts with the

[21] Bank of England, 2022, "Artificial intelligence and machine learning," DP5/22, https://tinyurl.com/47xds9dh
[22] Bank of England, 2023, "Response paper on artificial intelligence and machine learning," FS2/23, October 26, https://tinyurl.com/5bsua5b9
[23] Bank of England (n 21)
[24] PRIN 2.1 The Principles – FCA Handbook, https://tinyurl.com/4uh8yuh5
[25] PS22/9: A new Consumer Duty I FCA, https://tinyurl.com/bdev8k78

regulated business. As such, and insofar as the Principles are sufficiently broad, they will mitigate the risks in this specific context.

- The Principles are supported further by the FCA's Vulnerable Customer Guidance.[26] In practice, these complement the Principles and inform firm's behavior in complying with their obligations in respect of vulnerable persons.
- The Duty serves to increase the responsibilities inferred on firms under the Principles; in essence, it requires that firms have a greater responsibility and "more positive role in delivering good outcomes for [retail] consumers" beyond their clients.[27]

Further, legislation such as the Equality Act 2010 will apply to prohibit instances of discrimination; the Vulnerable Customer Guidance expressly notes that firms should have regard to the 2010 Act and aims to implement similar outcomes to the anticipatory duty on reasonable adjustments. Many of the protected characteristics overlap between the Guidance and 2010 Act, meaning that a breach of one will likely result in a concurrent breach of the other.

5.2 Data processing

In practice, AI systems will process significant quantities of data when fulfilling the set functions. Such data may, and likely will, include "personal data" as defined by Regulation (EU) 2016/679 (the 'GDPR'). Where personal data is processed as part of the activities of an E.U. entity, it must be done in accordance with the GDPR;[28] in essence, the data processor must have a lawful basis for the processing of such data and it must implement proper procedures whereby the data subjects can exercise their rights.

The primary question centers on whom assumes the position of (and liability as) the data processor. In theory, the AI system could be considered to be the data processor insofar as it is responsible for processing such data. However, and as discussed above, AI does not have a separate legal personality and so cannot assume the responsibilities attributable to a data processor under the GDPR. Thus, the issue centers on whether the data processor will be the AI provider, developer, or the financial services organization adopting and utilizing the technology. In practice, this will be determined on a case-by-case basis. For example, where an organization opts for AIaaS the underlying service provider will likely be considered the data processor; on the other hand, where an organization has developed an in-house AI system, they will be considered the responsible party.

Irrespective of this, the principles and regulations within the GDPR will be applicable in this context. The factual circumstances and underlying risk remain the same; assuming the data processor can be properly identified, then the GDPR should prove efficient in addressing the issue of AI data processing.

6. DIRECT REGULATION

6.1 The E.U. AI Act

6.1.1 OVERVIEW AND APPLICATION

The E.U. is leading the way by being the first regulatory body to attempt to regulate AI, having approved a set of regulations to be applied to AI systems across Europe in early December 2023. The new rules are to be contained in the E.U. AI Act ("the Act"),[29] which is slated to take effect in early 2024. It will a broad application, applying horizontally across all sectors; additionally, it has been attributed extra-territorial effect, so will apply to any third-country providers and users of AI systems where such systems or generated output is used within the bounds of the E.U. In essence, it aims to unify and coordinate regulatory efforts across member states while minimizing the risks attributed to AI systems within the context of the E.U.

6.1.2 A RISK-BASED APPROACH

The Act adopts a risk-based approach, focusing on addressing and regulating AI systems that present the greatest "risk" while simultaneously clarifying the obligations of the AI providers and deployers. To expand, it categorizes AI systems according to risk, with more stringent regulations being applied to those that present the most significant risks to E.U. persons and values. In this sense, the Act applies to AI systems generally instead of creating rules for specific industry sectors.

[26] FG21/1: Guidance for firms on the fair treatment of vulnerable customers, https://tinyurl.com/23v5yw47

[27] Bank of England (n 21) at 4.9

[28] See the Data Protection Act 2018 for the U.K. transposition.

[29] 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, 8115/21, January 22, 2024.

It prohibits the categories of AI systems that are taken to present the greatest risk of causing harm; this includes exploitative and certain types of biometric identification system (e.g., emotion recognition and social scoring in various circumstances).[30] Such AI systems are deemed to create an "unacceptable" degree of risk insofar as they contravene E.U. values or constitute a sufficient threat to established fundamental rights. For example, developers and providers will not be able to put AI systems that would exploit specific vulnerabilities where the purpose of such exploitation is to materially distort the behavior of that person or group in a way that may cause significant harm on the market. Naturally, this acts to protect consumers insofar as financial services firms will not have access to such systems within the E.U. This may limit financial services firms from adopting such systems through AIaaS or external routes.

The Act also purports to limit the use of "high-risk AI systems" to narrowly defined instances that are subject to strict requirements.[31] Such AI systems will be deemed "high-risk" where they present "significant potential harm" to E.U. persons and their "health, safety, fundamental rights" or, more broadly, the "environment, democracy and[/or] the rule of law." In principle, it has been argued that the criteria adopted is sufficiently broad so as to encompass AI systems used to evaluate creditworthiness, grant loans, or facilitate other financial services activities. Accordingly, those who adopt such systems may need to adhere to the heightened obligations and regulatory burdens prescribed by the Act.

Irrespective of this, the E.U. has recognized that the test is sufficiently broad in its scope. As such, and to address borderline cases or potential compliance issues, providers must complete assessment documentation and registration documentation in an E.U. database before introducing the system to the E.U. market; the Commission will then determine whether the system presents a "high-risk" or would fall within a lower-risk category (as discussed below).

Where a system presents a "limited risk", the provider must still adhere to some compliance requirements, although they are less onerous than those attached to high-risk systems. Essentially, such providers will be required to inform users that the content or system is AI generated. Where AI presents an even lower risk, providers are not obligated to adhere to any compliance efforts; rather, they are simply encouraged to implement voluntary codes of conduct and practice.

6.1.3 SYSTEMIC RISK

As noted, issues of systemic risk are addressed in the regulations addressing general-purpose AI (GPAI) models;[32] this essentially refers to AI systems that show "significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed."[33] A GPAI model will attach systemic risk where it has "high-impact capabilities".[34] Providers of such models will be required to maintain up-to-date technical documentation and they must make any such information available to providers that integrate the AI in their systems.[35] Further, they must make information pertaining to the content used to train the AI system publicly available.[36] These obligations are accompanied by other monitoring and procedural requirements,[37] all of which address the concerns surrounding a lack of transparency and insufficient oversight. To this end, the Act addresses some of the primary risks attributable to the integration of AI systems in financial services, thereby removing barriers to its utilization.[38]

6.1.4 RIGHTS AND OBLIGATIONS

Put simply, the Act distinguishes between the obligations borne by providers or developers and those borne by users. In practice, financial services firms are likely to be considered users rather than developers; however, it may be possible that a financial services firm becomes a developer should it develop its own AI system. Providers and developers must: ensure AI systems are transparent; inputted data is of a sufficient quality and integrity; they are accountable for the system; and that they comply with technical standards required by the E.U. Users must conduct proper risk assessments and comply with proper monitoring efforts.

[30] EU AI Act, Title II.
[31] EU AI Act, Title III.
[32] EU AI Act, Article 52.
[33] EU AI Act, Article 3(44b).
[34] EU AI Act, Article 52(1), as defined in Article 22.
[35] EU AI Act, Article 52c(1).
[36] EU AI Act, Article 52c(1)(d).
[37] EU AI Act, Articles 52d and 52e.
[38] See section 3.2.2.

The Act does not, in itself, create individual rights for those harmed by AI systems in practice;[39] rather, it does clarify and codify the obligations of the relevant parties. Further, it seeks to promote transparency within AI systems and their adoption within various industries. For financial services institutions, evidencing decision-making processes and justifying decisions will necessitate that they are transparent about their efforts and structures irrespective of whether they are the provider or user. As discussed, the inherent lack of certainty as to the allocation of liability and issues of transparency have presented the primary barriers for the adoption of AI in all industries; as such, it is submitted that the Act provides much needed clarity in support of AI integration.

6.2 The E.U. AI Liability Directive

The E.U. AI Liability Directive ("the Directive")[40] aims to address potential claims for harm caused by AI systems. While at an earlier stage of the legislative process, it is intended to accompany the Act and the clearer obligations set out therein.

The Directive will apply to AI systems that are available to, or operate within, E.U. markets; in doing so, it shall act as a standard of minimum harmonization (i.e., persons may elect to invoke national laws where they appear more favorable), but will need to be transposed into national law. It seeks to address the shortcomings of traditional liability rules in addressing claims for harm against AI systems; as such, the proposals focus on addressing the difficulties of proof attaching to the complexities introduced by AI.[41] In doing so, the Directive aims to recognize the nuances of AI and, therefore, sets out a new evidentiary mechanism; this mechanism aims to address the lack of transparency and complexity associated with AI systems. In doing so, the Directive also aims to establish a presumption of causation between the defendant and harm complained of.

Thus, when read with the Act, the proposed procedural rules could alleviate some of the key barrier to corporate integration and adoption of AI insofar as it purports to clarify the extent and allocation of liability; however, at the time of writing, it remains subject to EU approval and, therefore, has no binding legal effect.

7. ETHICAL AI

"Ethical AI" requires that AI systems are developed, implemented, and used in ways that align with ethical standards, respecting established values and fundamental human rights. In doing so, ethical AI seeks to advance the transformative potential of AI systems while protecting human values and societal wellbeing. Achieving this in practice requires robust guidelines, with industry participants and policymakers agreeing to set principles. It is a critical component of any organizational strategy on AI.

Validate AI, an independent community interest company, focuses on improving the validation of AI and have developed a number of whitepapers and voluntary codes of conduct to this end. The most recent whitepaper has been the subject of wide engagement, setting out a framework that supports the widespread adoption of ethical AI.[42] To expand, the approach focuses on six fundamental pillars, with each addressing risks commonly associated with AI integration. The following sets out each of the pillars, highlighting how they serve the underlying aim of ethical AI:

(i) **Responsibility and accountability:** organizations should be held accountable for the consequences of the systems they develop, with this being central to the degree of risk attaching to the product. Validate AI suggest that developers should appoint an AI officer responsible for monitoring risks and managing the responsible deployment of AI systems.

(ii) **Code of practice:** codes of practice are central to ensuring that AI systems are deployed to certain standards; Validate AI submit that practitioner focused codes of conduct are required "to ensure that AI systems can be trusted."

(iii) **Convening:** convening and coordination are key to ensure all stakeholders are heard when considering the deployment and regulation of AI systems.

(iv) **Independent audit:** audits are viewed as particularly useful where high-impact AI systems are at issue insofar as they act to mitigate the likelihood that inappropriate, high-risk systems are deployed. This is common practice in other industries where public safety concerns are relevant.

[39] Cf. Section 6.2.
[40] EUR-Lex (n 8)
[41] See Section 3.2.1.
[42] 14072023 Validate AI – Our position to tackling AI risk, https://tinyurl.com/ya9zyzuk

(v) **Monitoring:** AI systems should be continuously monitored after deployment, with contingency plans in place to manage a number of scenarios. This educates relevant parties as to the nature of the specific AI system while providing protection against the risks of failure.

(vi) **Education:** educating industry participants, businesses, the general public, and governments about AI and the associated risks is key to ensuring those parties are able to properly assess and make informed decisions about AI systems they may interact with. Validate AI suggest that "education should be practitioner-centric," ensuring that industry participants can apply ethical standards in their development roles. Similarly, they suggest that general education can be tailored to the application of AI in different industries.

Together, these pillars act to promote fundamental values and improve the social responsibility in the adoption of AI, thereby mitigating the aforementioned risks and removing barriers to the development and implementation.

8. CONCLUSION

AI systems are valuable tools that can be applied in nearly any industry; they are of particular utility in the context of financial services, where the management and use of data has been the foundation of businesses since their inception.

It is, however, clear that some degree of regulatory intervention is required to enable the most efficient integration of the technology. The proper application of public policy and the specifics of regulation remain uncertain. While obvious, the need to balance innovation with safety is difficult to strike. Alongside this, international competitiveness has become a critical focus for policymakers and remains a significant challenge for businesses (particularly those that are cross-border in nature). However, financial services firms are familiar with these high-level questions and challenges; businesses are demonstrating an increased understanding of the benefits to be derived from AI systems and through engaging with fintech partners, suggesting these barriers are not insurmountable; from this, it is apparent that the adoption of industrial data processing and the use of novel AI systems will continue among the most successful financial services firms over the coming years.

This document was produced for information purposes only and is for the exclusive use of the recipient.

This publication has been prepared for general guidance purposes, and is indicative and subject to change. It does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (whether express or implied) is given as to the accuracy or completeness of the information contained in this publication and The Capital Markets Company BVBA and its affiliated companies globally (collectively "Capco") does not, to the extent permissible by law, assume any liability or duty of care for any consequences of the acts or omissions of those relying on information contained in this publication, or for any decision taken based upon it.

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy focused in the financial services industry. Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC

Bengaluru – Electronic City
Bengaluru – Sarjapur Road
Bangkok
Chennai
Gurugram
Hong Kong
Hyderabad
Kuala Lumpur
Mumbai
Pune
Singapore

MIDDLE EAST

Dubai

EUROPE

Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
Glasgow
London
Milan
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA

Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto

SOUTH AMERICA

São Paulo

WWW.CAPCO.COM

CAPCO
a wipro company