AIFS0082

Written evidence submitted by Anna Katsoulaki

Lecturer in Law and PhD candidate at Cardiff University, School of Law and Politics.

Submitting evidence on:

'How can Government and financial regulators strike the right balance between seizing the opportunities of AI but at the same time protecting consumers and mitigating against any threats to financial stability?

This may include:

Are new regulations needed or do existing regulations need to be modified because of AI?

Will Government and regulators need additional information, resources or expertise to help monitor, support and regulate, AI implementation in financial services?'

Summary

AI technologies offer transformative potential for UK financial services but they also introduce new risks that must be managed. This submission addresses how government and financial regulators can strike the right balance between seizing the opportunities of AI and protecting consumers while safeguarding financial stability. It finds that the UK's current regulatory framework relies on existing rules and principles and has favoured legal oversight. While this encourages innovation, it can have the opposite results, with ambiguity about AI governance deterring banks and fintechs from investing in cutting-edge AI tools due to uncertainty, compliance fears, and cost concerns. In the dilemma innovation v. regulation, stronger targeted regulation of AI where needed, might be the right answer that will not undermine innovation, as perceived.

Key conclusions and recommendations include:

Need for clear and updated regulation

Existing laws (e.g. data protection, financial conduct rules) only partially address AI-specific challenges, such as algorithmic transparency and bias. Without clarity, firms face a Catch-22: innovate and risk breaching unclear rules, or hold back and miss AI's benefits. New regulations or updates to existing ones are needed to provide certainty and to require robust AI oversight.

Ameliorate regulatory capacity and coordination

Government and regulators (FCA, PRA, ICO, etc.) require enhanced expertise, resources, and coordination mechanisms to effectively monitor AI in financial services. Joint efforts –

such as the FCA/ICO's new AI innovation roundtable – are a positive step to ensure consistent guidance. Investment in specialist staff and 'RegTech/SupTech' tools will help regulators keep pace with industry AI adoption. Close collaboration with the industry is of paramount importance too.

Introduce an 'AI in Finance Act'

Parliament should strongly consider a dedicated AI in Finance Act, modelled in part on the EU's risk-based AI Act, to future-proof the UK's financial regulations. This Act would set sector-specific rules for AI, particularly high-risk uses like anti-money laundering (AML) systems and Suspicious Activity Reporting (SAR). It should define clear obligations proportionate to a firm's size and AI risk exposure (e.g. requirements for testing, explainability and governance corresponding to the scale of the firm, considering SMEs) and formalise safe innovation practices such as regulatory sandboxes. This would establish legal accountability and fines for AI-related compliance failures; note that already banks are paying large fines for failing to trace money laundering and AI use will help them avoid being in this situation possibly. This framework would encourage ethical innovation by removing uncertainty, ensuring firms can invest in AI with confidence.

Promote ethical AI to enhance financial crime prevention

With clear guidance and oversight, AI can be a powerful ally in protecting consumers and the financial system. For example, AI-driven analytics can filter massive transaction datasets to flag fraud and money laundering patterns far more accurately and quickly than traditional systems. This can reduce the burden of false positives in SARs and free up human experts to focus on truly suspicious cases. However, to achieve these benefits, firms need assurance that using AI is encouraged within a well-defined risk management framework, not a regulatory grey zone. A balanced approach with explicit rules, rigorous oversight, and support for innovation will enable the UK to use AI for financial good (e.g. faster crime detection, better consumer outcomes) while minimising harms (like biased decision-making or systemic risks from untested models).

In summary, the UK should move beyond the wait-and-see-how-AI-will-be-used-by-the-private-sector approach of recent years and adopt a pro-innovation and proactive-regulation strategy. By updating its regulatory architecture (potentially via a new Act) and investing in regulatory capabilities, the UK can provide much-needed clarity. This will unlock AI's opportunities in finance – such as smarter AML compliance, improved fraud prevention, and more inclusive services – in a manner that protects consumers and the stability of markets. The following sections elaborate on the current landscape, identified gaps, and detailed recommendations for Parliament's consideration.

Introduction

AI is becoming increasingly essential to financial services, offering capabilities to analyse data, detect patterns, and automate decisions with unprecedented speed. In the UK, two-thirds of financial firms report using machine learning (ML) in some form, across front-office and back-office functions.[1] Notably, anti-money laundering (AML) and fraud detection are among the most common use-cases for AI/ML in finance.[2] This is unsurprising since the scale of modern financial crime demands technological assistance. Money laundering in particular is related to some of the worst crimes like putting vulnerable people at risk, modern slavery / human trafficking, supply of firearms and illegal drugs, organised immigration crimes.[3] The annual cost of money laundering to the global economy is staggering, with estimates suggesting losses ranging from 2% to 5% of the world's GDP, or approximately $800 billion to $2 trillion USD.[4] British banks spend over £5 billion annually on financial crime compliance (more than the UK's prison budget)[5], yet the system struggles with efficiency. In the year 2022/23, the UK's Financial Intelligence Unit received approximately 859,000 suspicious activity reports (SARs), an enormous volume that is found to be unmanageable.[6] A large proportion of these SARs are generated by banks' automated transaction monitoring alerts, many of which turn out to be false positives or low-quality leads and this creates "quantity over quality" issues.

AI-enhanced systems present an opportunity to shift this paradigm. Advanced algorithms can learn complex patterns of illicit behaviour, correlate information across accounts and datasets, and update faster than current systems. For example, AI can scan millions of transactions in real-time to spot anomalous behaviour that a human might miss or evaluate whether photos in different identity documents match.[7] It can also cut down duplicate or false alerts. In practice, this means compliance teams could be alerted to truly suspicious activities with greater accuracy, focusing investigative effort where it matters, saving time and costs. Recent FATF analysis acknowledged that AI and other new technologies could dramatically improve the speed and quality of AML measures – if implemented responsibly.[8] The UK's ongoing SARs Reform Programme similarly aims to 'modernise the technology used for SARs reporting and analysis' to help law enforcement better utilise intelligence from the private sector.[9]

---

[1] https://www.fca.org.uk/publication/research/research-note-on-machine-learning-in-uk-financial-services.pdf, at p.3
[2] Ibid.
[3] Nic Ryder
[4] The Impact of Artificial Intelligence in Anti-Money Laundering - European Institute of Management and Finance
[5] Using artificial intelligence to keep criminal funds out of the financial system | FCA
[6] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/710-sars-annual-statistical-report/file, at p.4
[7] https://www.fsb.org/uploads/P011117.pdf, at p.20
[8] Opportunities and Challenges of New Technologies for AML/CFT
[9] https://assets.publishing.service.gov.uk/media/642561b02fa8480013ec0f97/6.8300_HO_Economic_Crime_Plan_2_v6_Web.pdf, at p.28

However, the adoption of AI in finance also introduces risks and uncertainties. Unlike traditional software, many AI/ML models function as 'black boxes' whose decision logic is not easily interpretable.[10] This opacity can conflict with regulatory expectations for firms explainability on their decision-making (whether declining a transaction or refusing a customer) and makes it harder for regulators to trust AI-driven outcomes. There are also concerns around data privacy and bias. AI systems trained on historical data might inadvertently perpetuate discrimination or unfair bias in credit, fraud, or AML decisions. Misuse of AI could lead to consumers being wrongly denied services or incorrectly flagged as high-risk, undermining trust and potentially breaching data protection or equality laws. In the worst case, unchecked deployment of AI in trading or risk management could pose threats to financial stability; for instance, if many firms rely on similar self-learning algorithms that behave unpredictably under stress, or if a major institution's AI system fails in a critical task. Note that human intervention is necessary to effectively use AI in times of severe unpredictability, otherwise the AI will produce false results. Is such cases and times, financial instability will be directly connected to the use of AI.

The above pose the following question: Does the current UK regulatory and legal framework adequately address the novel challenges of AI in financial services, or are new measures required? And do regulators have the tools and expertise to both encourage beneficial innovation and guard against AI-driven harms? The remainder of this evidence examines the UK's existing approach, compares it with international developments (notably the EU's AI Act and global AML standards), identifies gaps and risks, and proposes recommendations to ensure that the UK achieves a sensible balance between innovation and protection in the age of AI.

Legal and policy landscape in the UK

The current legal framework has mainly supported pro-innovation principles and existing relevant laws around AI. Policy under the Conservative government championed a 'pro-innovation, light-touch' approach across sectors.[11] A 2023 White Paper[12] on AI regulation set out broad principles – like safety, transparency, fairness, accountability – to guide how existing regulators oversee AI in their domains, rather than creating a single new AI law. The Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA), Information Commissioner's Office (ICO) and others were expected to integrate these principles into their supervision using their current powers. In financial services, this means AI is largely governed today by general obligations in laws such as the Financial Services and Markets Act 2000, the Money Laundering Regulations 2017 (as amended), and UK GDPR/Data Protection Act 2018 – without explicit reference to AI.

[10] Supra at n.4
[11] Establishing a pro-innovation approach to regulating AI - GOV.UK
[12] A pro-innovation approach to AI regulation - GOV.UK

Banks and firms must ensure effective risk management and internal controls (under FCA/PRA rules), which would involve control of any AI models they adopt. The PRA's recent guidance on Model Risk Management (SS1/23) applies to all models, including AI/ML, requiring firms to validate models and govern their use.[13] Similarly, Senior Managers and Certification Regimes (SM&CR) hold named executives responsible for a firm's controls and this includes AI systems. Furthermore, the UK's data protection laws impose duties relevant to AI, such as transparency, data minimisation, and conducting Data Protection Impact Assessments[14] for high-risk processing including some AI profiling. The ICO has issued detailed Guidance on AI and Data Protection, clarifying how fairness and transparency principles apply to AI systems.[15] For instance, if a bank uses an AI system to screen transactions or customers, it must process personal data in a way that is transparent.[16] Finally, equality and consumer protection laws also apply. The Equality Act 2010 would hold a firm liable if its AI system unlawfully discriminates against protected groups in lending or fraud detection. The FCA's new Consumer Duty[17] (in force 2023) mandates firms to deliver good outcomes for customers, which means they should ensure AI-driven decisions (like credit refusals or fraud blocks) are not causing foreseeable harm or unfair outcomes.

In theory, these existing regulations do cover many aspects of AI risks. Indeed, a 2019 joint Bank of England–FCA survey[18] found 75% of UK financial firms did not view regulation as an 'unjustified barrier' to ML deployment. However, the same survey noted that some firms struggled with uncertainty and they cited "a lack of clarity and uncertainty around how existing regulations apply to ML", especially regarding model explainability and oversight of AI 'black boxes'. Firms indicated that additional guidance would help them interpret regulators' expectations and design appropriate controls for AI. In other words, while no one is asking to weaken core rules, there is recognition that applying old rules to new tech isn't straightforward. In addition, a March 2025 FCA and Bank of England letter to Trade Association chairs and CEOs discusses about again about surveys that 'appear to demonstrate a lack of confidence amongst some firms to develop and adopt AI technology, as well as potential uncertainty around the interactions between our regulatory regimes'.[19]

Under the former Conservative Government, the philosophy was that bespoke AI legislation was premature and it would be better to encourage innovation under watchful eyes than risk putting constraints on it. However, there is potential a shift with the new Labour Government. The current government have signalled greater concern about AI's risks and a willingness to introduce targeted, binding regulations where necessary. Labour's 2024 Manifesto[20] pledged to "ensure the safe development and use of AI models by introducing binding regulation on the handful of companies developing the most powerful AI models". This might indicate a move away from a purely laissez-faire stance. Still, Labour's approach is not to regulate AI

[13] FS2/23 – Artificial Intelligence and Machine Learning | Bank of England
[14] Data Protection Impact Assessments (DPIAs) | ICO
[15] Guidance on AI and data protection | ICO
[16] How do we ensure transparency in AI? | ICO
[17] https://www.fca.org.uk/publication/policy/ps22-9.pdf
[18] https://www.fca.org.uk/publication/research/research-note-on-machine-learning-in-uk-financial-services.pdf
[19] https://www.fca.org.uk/publication/correspondence/fca-ico-joint-letter.pdf
[20] https://labour.org.uk/change/

across the board, but rather to focus on specific high-risk areas. Notably, Labour proposes a new Regulatory Innovation Office to coordinate and speed up regulators' responses to emerging tech; an idea aimed at improving cross-sector expertise and guidance, rather than creating an entirely new AI regulator. In practice, for financial services, this could mean more direction on how the FCA and PRA should approach AI.

At present, no dedicated financial AI law exists in the UK. In late 2023, the Financial Services and Markets Act 2023 was passed to update post-Brexit regulatory frameworks; it included new secondary objectives for growth and competitiveness that encourage regulators to facilitate innovation (implicitly including AI) in a safe manner. And in early 2024, the Government launched an AI Security Institute focusing on advanced AI risks, albeit more on societal and existential risks than financial sector specifics. Meanwhile, regulators like the FCA have been proactive in soft ways: the FCA ran 'TechSprint' hackathons and pilots on AI for AML and fraud detection, established an AI regulatory 'sandbox' through the Digital Sandbox initiative, and even set up an internal AI Department/Lab to build their knowledge . These efforts demonstrate that within the current legal landscape, there is support for innovation through supervision, but also a possible acknowledgment that more formal rules or guidance may eventually be needed as AI becomes necessary. As the next section shows, this question of new regulation is being heavily influenced by international developments, especially in Europe.

International, EU and UK regulatory approaches

The UK hitherto has opted for regulator-led, principle-based governance of AI in finance. Regulators like the FCA and PRA are leveraging existing tools – for instance, extending model governance expectations and conducting thematic reviews. The Bank of England/FCA ‘‘AI Public-Private Forum" (AIPPF) delivered a major report in 2022 examining AI risks in financial services, which helped inform regulators' thinking. In October 2022, the authorities issued Discussion Paper DP5/22 on AI and Machine Learning, inviting industry input on whether regulation needs to adapt. Industry feedback (summarised in a 2023 Feedback Statement) echoed calls for coordination and clarity: respondents noted the UK's regulatory landscape for AI is complex and fragmented, and they urged better alignment between domestic regulators and with international norms . Many suggested a risk-based approach to defining AI (focusing on harms rather than a rigid definition) and 'live' guidance that can be updated as the technology evolves. Importantly, respondents largely felt that existing governance frameworks like SM&CR can cover AI risks if applied properly, though certain AI-specific issues (e.g. data bias, algorithmic accountability) might need stronger or clearer requirements.

To address innovation, UK regulators have used sandbox environments and guidance. The FCA's Regulatory Sandbox and Digital Sandbox have allowed firms to test AI-driven

services (such as AML pattern-detection algorithms) under regulatory oversight. The ICO and FCA have also collaborated, recognising that confusion about overlapping regulations (financial vs data protection) can chill innovation. In March 2025 they jointly announced an industry roundtable to discuss regulatory uncertainty around AI, noting concern about a 'lack of confidence among some firms to develop and adopt AI technology' due to unclear interplay of rules. This kind of regulatory cooperation (under the umbrella of the Digital Regulation Cooperation Forum (DRCF)) is an attempt to present a unified front and clarify expectations for industry. However, these efforts remain largely informal or experimental. They do not carry the force of law or binding rules specific to AI in finance.

In contrast, the EU has drafted the Artificial Intelligence Act, a horizontal regulation that will impose binding requirements on AI systems, including those used in financial services. The AI Act employs a risk-tiered approach: it bans a few 'unacceptable risk' uses outright, designates certain uses as 'high-risk' (subject to strict compliance controls), and lightly regulates limited-risk AI (transparency obligations for things like chatbots). Notably, many AI applications in finance are likely to be classified as high-risk under the EU AI Act because of their potential impact on individuals' rights and the financial system. The European Commission has signalled that AI used in credit scoring, fraud prevention, customer due diligence and transaction monitoring will likely be treated as'high risk' AI systems. This means banks and fintechs deploying such AI tools in the EU will have to meet a range of stringent requirements: risk management systems, rigorous testing and validation, ensuring high quality of training data to minimise bias, detailed technical documentation, human oversight, and robust transparency/explainability mechanisms. For example, Article 10 of the draft EU Act requires that providers of high-risk AI (such as a transaction monitoring system) use appropriate training, validation and testing data governance measures to ensure the system is effective and fair.

The EU AI Act also mandates that Member States establish regulatory sandboxes for AI, to encourage experimentation under supervision, and it introduces hefty penalties for non-compliance. Fines can reach up to €35 million or 7% of global turnover (whichever is higher) for the most serious violations (e.g. using prohibited AI systems), with tiered lower fines (e.g. 4% or 2% of turnover) for lesser infringements . This penalty regime is intentionally akin to the EU GDPR fines, underscoring how seriously AI obligations will be taken. The EU's approach is therefore more prescriptive and enforceable than the UK's current stance, although it too incorporates proportionality (for instance, small and medium enterprises face the fine at the lower fixed amount rather than the percentage in some cases) .

For financial institutions operating across borders, the EU AI Act is a game-changer. A UK bank with EU customers or affiliates will be subject to those rules, effectively raising its compliance bar. International firms might adopt EU-level controls globally for consistency (the Brussel's Effect). This dynamic creates pressure on the UK either to align to some degree or risk divergence. It is noteworthy that EU lawmakers explicitly included financial crime prevention tools in their scope: AI used for money laundering detection would almost certainly be high-risk and expected to have human oversight. Commentators have observed

that many requirements in the AI Act for high-risk systems mirror existing expectations of regulators like BaFin or the FCA (e.g. having effective model governance and risk controls). In other words, complying with the AI Act might not be a radical departure for well-run financial institutions, but it will formalise and standardise those practices across the single market.

On the international stage, bodies like the Financial Action Task Force (FATF) have been examining AI within the context of AML/CFT. FATF's 2021 report 'Opportunities and Challenges of New Technologies for AML/CFT' praised the potential of AI and machine learning to improve risk detection and compliance efficiency. It gave real examples – e.g. using machine vision to match faces on ID documents, or ML algorithms to better identify high-risk customers – showing that when responsibly implemented, such tech can strengthen the AML regime. However, FATF also noted key obstacles that cause industry hesitancy in adopting AI: banks fear regulatory criticism or even punitive action if an AI pilot fails or reveals gaps in their existing controls, and they worry that introducing innovative techniques could lead regulators to raise the compliance bar further. Essentially, firms are concerned they'll be 'punished for innovating' – a theme also echoed by UK Finance and other industry groups. FATF recommends that supervisors actively engage and reassure industry, perhaps via guidance or sandbox programmes, to deal with these fears. This aligns with steps UK regulators are taking (e.g. the FCA's regulatory Sandbox and TechSprints, and the current FCA-ICO industry roundtable aimed at providing clarity).

In summary, the EU's emerging AI Act provides one model – a comprehensive, cross-sector law with explicit rules – while the UK so far has preferred flexibility, relying on existing laws plus guidance. FATF urges a balanced risk-based approach. The UK now faces a strategic choice: whether to stick with incremental adjustments or pivot to a more codified regime for AI in finance. The next section evaluates where the current approach might fall short and what risks need addressing.

Analysis of gaps and risks

The evidence indicates several gaps in the current UK approach that could impede both innovation and consumer protection if not addressed.

Perhaps the clearest gap is the lack of certainty and explicit rules regarding AI use. Firms may be unsure how far they can go in automating decisions or monitoring using AI without running into compliance trouble. As noted, many firms have called for clearer guidance on how existing rules apply to AI. The joint FCA-ICO letter (March 2025) acknowledged a "lack of confidence" among firms about AI adoption due to perceived regulatory grey areas. When in doubt, many firms take a conservative path – either not deploying advanced AI, or limiting

its functionality (e.g. using a simpler, more explainable but less powerful tool to satisfy regulators). This means consumers and the financial system may be missing out on beneficial innovations – such as more accurate fraud detection or personalised services – because firms fear regulatory backlash from using more cutting-edge AI. Moreover, smaller fintech startups face a cost barrier: navigating unclear compliance expectations requires legal spend and risk assessments that can stifle a new entrant. A well-defined framework would reduce these frictional costs and uncertainties.

While existing regulations cover general principles, they may not explicitly require best practices for AI. For instance, there is currently no UK regulation that plainly requires firms to conduct bias testing on AI models or mandates explainability standards for AI in finance. One firm might voluntarily do intensive model validation and bias audits, while another might not – and unless an incident occurs, the latter might not be scrutinised. This inconsistency can lead to uneven consumer protection. If, say, one bank's AI mortgage approval system inadvertently disadvantages certain minorities due to training data bias, it could go undetected if the bank isn't proactively checking and regulators haven't set clear expectations. Similarly, transparency to consumers about AI-driven decisions (such as being flagged in a fraud risk model) is not clearly mandated beyond the broad GDPR provisions, which aren't tailored to financial contexts. Without specific rules, there is a risk of harmful or unethical AI practices slipping through under the radar.

On the regulator side, overseeing AI models is challenging. Financial regulators historically focused on processes and outcomes, but now they might need to inspect algorithmic code, data sets, and ML training processes – areas that demand data science expertise. The ICO has built significant AI expertise (publishing an AI risk toolkit, etc.), and the FCA is ramping up its internal data and AI units, but these efforts need to scale. The Digital Regulation Cooperation Forum is a useful mechanism for sharing knowledge among UK regulators (FCA, ICO, Ofcom, CMA) on AI issues . Still, as AI proliferates, regulators may be stretched thin in reviewing models across hundreds of firms. This raises a risk of inadequate oversight – either supervisors missing problems due to lack of skill or bandwidth, or slowing down approvals for new AI applications due to backlog, thus delaying consumer-benefiting innovations. The Government may need to ensure regulators have funding to recruit AI specialists and develop SupTech (supervisory technology) to automate some oversight tasks.

Focusing on the AML/SARs domain, the current ambiguity carries a double-edged risk. On one side, banks might under-invest in AI analytics, sticking to outdated transaction monitoring systems that produce the familiar flood of SARs. This 'status quo bias' leaves known inefficiencies in place, contributing to continued low conversion rates of SARs to actual enforcement outcomes and high compliance costs for industry. (It is telling that despite nearly 900k SARs filed annually, the amount of assets actually restrained from criminals, while significant (£300m+ in 2021/22), suggests a small fraction of SARs lead to action.[21] Improving quality through AI could help, but banks may hold off without guidance or

safe harbour assuring them that new methods are acceptable.) On the other side, if firms do deploy AI without clear standards, there's risk they over-rely on technology without proper controls, potentially leading to blind spots. For example, a poorly supervised AI could learn to ignore certain typologies of crime because they were rare in training data, thus missing novel forms of illicit finance – a serious threat to law enforcement goals. Or it might flag so many transactions as suspicious (due to an overly broad pattern match) that human investigators are overwhelmed – a different sort of failure. The current law (Money Laundering Regulations) requires firms to have systems to detect and report suspicious activity, but says nothing about acceptable false positive rates or interpretability of those systems. This lack of specificity becomes more important as AI systems get complex. In short, the absence of explicit AML AI guidelines may either slow adoption or foster risky implementations, both of which undermine the ultimate objective of fighting financial crime effectively.

While consumer protection has been vital, there's also the question of financial stability – the Treasury Committee's question explicitly includes mitigating threats to stability. Could AI usage threaten stability? In retail banking/AML, it's unlikely to be systemic in itself (though successful money laundering unchecked at scale can have societal costs). The UK might consider whether to explicitly require firms (especially systemically important ones) to obtain independent validation of critical AI systems' robustness. Again, it is important to remember that AI can not be relied in cases of stress and uncertainty, like pandemics etc. Stability can be influenced if trust is lost following a few stress periods that go unchecked.

Another issue is the divergence with the EU. If the UK does nothing new while the EU implements the AI Act, UK-based firms could face a more burdensome regime abroad than at home. This might make the UK market a relative haven for AI experimentation – which could be positive for innovation or negative if it attracts lower standards. It could also complicate compliance for firms straddling both jurisdictions. The gap here is strategic: does the UK want to remain 'light-touch' to attract AI firms, or align with a more ethical approach to protect consumers similarly?

These gaps collectively suggest that while the UK's current approach has advantages (flexibility, encouraging innovation), it may not be sustainable or sufficient as AI becomes pervasive. The next section outlines concrete recommendations to close these gaps – most prominently, the proposal for an AI in Finance Act – and to strengthen the UK's ability to both foster AI innovation in finance and guard against its pitfalls.

Recommendations

[21] Supra at n.9

AIFS0082

1. Enact an “AI in Finance Act” – a sector-specific AI regulatory framework.

Parliament should consider introducing a dedicated “AI in Finance Act”, providing a clear legal foundation for AI oversight in financial services. This would not mean abandoning the pro-innovation ethos, but rather operationalising it through smart regulation.

Following the model of the EU AI Act, the law should categorise AI applications by risk criticality. For high-risk AI in finance (such as AML/SARs systems), the Act should mandate specific controls: robust validation before deployment, ongoing performance monitoring, documented explainability methods, bias testing, data quality standards, and human-in-the-loop oversight for critical judgments.

To avoid overburdening smaller firms and to reflect that large institutions pose bigger systemic risks, the Act should incorporate proportionality by firm size/scale. For instance, a global bank using AI for AML might be required to have an internal AI Ethics Committee, periodic independent audits of their AI models, and dedicated senior management functions accountable for AI governance. In contrast, a small fintech could comply through more streamlined measures.

To directly tackle the ‘fear of trying new tech' obstacle, the Act should formalise AI Sandbox programs. Building on the FCA’s successful sandbox, it could require that the FCA, PRA, and ICO jointly operate an “AI in Finance Sandbox” where firms can test AI-driven products (like a new transaction monitoring AI) with real data under supervision, without immediate threat of enforcement if things go wrong – as long as issues are remedied. The Act might grant regulators the authority to waive or modify certain requirements temporarily for testing purposes, and crucially, provide a limited safe harbour from regulatory sanctions for pilots conducted in the sandbox. In return, firms would need to share test results and lessons learned with regulators, contributing to collective learning. Such provisions would implement FATF’s advice for regulators to engage and encourage adoption of new technologies. It would give comfort that innovating won’t lead to punitive action so long as it’s done responsibly and transparently in cooperation with the regulators.

The Act should embed AI governance into firms’ obligations. For example, it could extend the Senior Managers & Certification Regime (SM&CR) to explicitly cover AI oversight – perhaps by requiring that a senior manager (such as the Chief Risk Officer or an innovation director) be designated responsible for the compliance of AI systems. Additionally, the Act could instruct regulators to develop guidance on AI transparency to consumers – e.g. requiring firms to inform customers when significant decisions are AI-influenced and how they can request human review (similar to GDPR Article 22 rights, but tailored to financial contexts). Ensuring consumers are not lost in the equation is vital for maintaining trust.

The Act should authorise regulators to impose meaningful penalties for breaches of the AI-related duties. This could be modelled on existing financial penalty regimes. For instance, if a firm deploys an AI system in a high-risk role (like AML monitoring) without due testing or oversight and it leads to a serious compliance failure, regulators might levy fines analogous to AML failings. Currently, banks have been fined tens of millions of pounds for AML systems failures under existing rules; the Act could clarify that failures specifically attributable to negligent AI governance will be met with similar gravity.

Overall, an AI in Finance Act would fill the policy vacuum with clear rules of the road. Far from hindering innovation, well-crafted regulation can catalyse innovation by erasing uncertainty. Firms will invest in AI once they know the rules and have confidence that by following them, they won't later be accused of missteps. Industry thrives on certainty. A good example is the UK's early clarity on fintech regulations that helped London become a fintech hub. Similarly, clarity on AI can make the UK a leader in "responsible AI in finance." Parliament taking initiative here would show international leadership, as few countries yet have sector-specific AI laws. It would demonstrate that the UK can be both pro-innovation and pro-consumer in the digital economy.

2. Strengthen regulators' capabilities and coordination.

Regulation on paper is only as good as its implementation. Therefore, alongside any new law, the Government must ensure regulators are equipped to enforce and support it.

The FCA, PRA, Bank of England and ICO should receive dedicated funding (potentially via an increase in levy on industry, which is justified if it enables more effective supervision benefiting the market) to hire data scientists, AI engineers, and domain experts. Every major financial regulator should have an internal AI & analytics unit that can inspect firm algorithms, reproduce results, and understand technical documentation.

The Government should encourage (or mandate via the recommended Act or other policy instrument) that regulators issue joint guidance on AI in financial services. A practical step would be a cross-regulator Code of Practice on Financial AI, covering expectations on issues like explainability, data management, fairness and consumer communications.

The success of the FCA's sandbox in fostering fintech innovation is well noted. These should be expanded for AI solutions, with continued involvement of multiple regulators (FCA, ICO, Payment Systems Regulator, etc. as relevant). The sandbox can also be a forum for regulators to learn hands-on about new AI tech. A formal annual 'AI and Financial Crime TechSprint' could be instituted, convening banks, fintech companies to collaboratively develop and test advanced AML AI tools, under the eye of regulators and law enforcement. This not only spurs innovation but builds trust between innovators and authorities.

3. Enhance legal clarity in existing frameworks through short-term adjustments.

While working on an AI in Finance Act may take time, there are interim steps that can be taken.

The Treasury, which has the ability to amend the MLRs via secondary legislation, could insert provisions related to technology. This would directly answer the question whether existing regulations need modification. They can be modified to explicitly acknowledge AI. The goal is to signal that using AI in AML is acceptable (even encouraged) if done responsibly, and here is what “responsible” entails.

The FCA could use its rule-making powers to create a section in the FCA Handbook on “Algorithmic Systems & AI”. The precedent exists in areas like algorithmic trading (where the Markets in Financial Instruments regime imposes specific systems and control requirements for algorithms). The FCA might not need to wait for new primary legislation to articulate expectations. A Policy Statement or Guidance could outline that firms using AI for customer decisions should be able to explain outcomes to the FCA upon request, should have proportionate governance, should notify the FCA of any material incidents caused by AI, etc.

4. Foster industry standards and accreditation.

Government and regulators can encourage the industry to develop self-regulatory standards for AI in financial services, which can complement formal regulation. For example, support could be given to industry bodies (like UK Finance, the Association of British Insurers, fintech associations) to create a Code of Conduct for AI in Finance. This could cover ethical principles, technical standards (e.g. suggesting use of model cards, bias audits, and explainability toolkits), and information-sharing on emerging threats (like fraudsters exploiting AI weaknesses).

Another concept is developing a certification schemes for AI systems used in finance. Accredited third parties (perhaps audit firms or specialised tech auditors) could evaluate an AI solution against defined criteria (accuracy, bias, security, etc.) and certify it. This could be especially useful for vendor-provided AI tools that many banks use.

5. Continue international engagement and alignment.

Finally, the UK should remain actively engaged with international bodies on AI in finance. Endorsement of FATF's recommendations on digital transformation should be followed by implementing them domestically. The UK should also monitor how other jurisdictions proceed – for instance, some US regulators are exploring algorithmic accountability in credit scoring, and Singapore/MAS has released principles for Fair and Ethical AI in banking (FEAT principles). Aligning with such initiatives can help UK firms operate globally with less friction.

In relation to the EU AI Act, the UK might not copy the entire EU Act, but it could still adopt its spirit for high-risk AI. The recommended AI in Finance Act could itself borrow heavily from the EU's proven provisions, adapted for UK context – thereby benefiting from years of EU deliberation

Conclusion

The rise of artificial intelligence in financial services is a pivotal development that the UK must both harness and control. The opportunities of AI – faster and smarter fraud detection, streamlined customer interactions, cost efficiencies, and even bolstering financial inclusion through better risk modelling – are enormous. Yet, these benefits will only materialise if consumers, firms, and regulators have trust in AI systems' fairness, transparency, and safety. Achieving this trust requires a balanced regulatory response: neither a hands-off approach that leaves dangerous gaps, nor an overbearing regime that smothers innovation.

The evidence highlighted in this submission – from industry surveys, regulatory feedback, and international comparisons – shows a clear demand for greater clarity and updated rules to govern AI's use in finance. The Government and regulators have an opportunity to proactively shape this next chapter of fintech progress. By enacting a targeted AI in Finance Act, supporting it with strong regulatory capacity and guidance, and aligning it with global standards, Parliament can ensure the UK remains at the forefront of both innovating with AI and regulating AI.

Such steps will remove the current 'fog' of uncertainty that hovers over financial AI deployments, thereby empowering banks and fintechs to invest in cutting-edge AI tools for financial crime prevention and customer service, with confidence. Clear rules and expectations will channel innovation toward ethical, accountable AI that serves consumers and stability. In parallel, those same rules will provide regulators the leverage to act decisively against any misuse – protecting consumers from harms like unfair bias or fraud, and protecting markets from systemic tech failures. It is a win-win proposition: thoughtful regulation as the foundation for sustainable innovation.

The UK can strike the right balance by moving from high-level principles to concrete, enforceable standards for AI in financial services, while continuing to seize the opportunities of this technology. With an appropriate regulatory framework in place, the UK's financial sector can confidently embrace AI to enhance its services and resilience, maintaining its global competitive edge and upholding the highest standards of consumer protection and financial integrity. The balance can and should be struck to secure the benefits of AI for the UK's economy and society while guarding against its risks.

April 2025