AIFS0059

Written evidence submitted by techUK

About techUK

techUK represents the companies and technologies that are defining today, the world that we will live in tomorrow. The tech industry is creating jobs and growth across the UK. Over 1,000 companies are members of techUK. Collectively, they employ more than 700,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new and innovative start-ups. The majority of our members are small-and medium-sized businesses. It should be noted that techUK is responding to this Call for Views on behalf of its members.

Executive Summary

AI is transforming financial services. Firms are using it to enhance operational efficiency, customer experience, and innovation. Key trends include the rise of large language models and AI-driven automation. AI is reshaping back-office operations such as fraud detection and process automation and is set to expand into front-office functions. Financial institutions are currently exploring advanced use cases like agentive AI, shallowfake detection, and AI-augmented software development.

AI is enhancing productivity, fraud detection, and regulatory compliance. It automates routine tasks, improves risk management, and enhances personalisation. AI adoption faces some barriers, including legacy infrastructure, data quality, and regulatory uncertainty. With a strong regulatory framework, skilled workforce, and flexible innovation environment, the UK is well-positioned to lead in AI adoption but investment in infrastructure and upskilling will be key.

AI does not pose unique risks to financial stability, its integration across financial services introduces challenges which can be monitored by industry. AI enhances cybersecurity by detecting fraud and supports digital resilience through verification with KYC/AML standards. The AI landscape is diverse, with the right infrastructure and oversight AI can be a powerful tool for innovation.

AI can enhance consumer outcomes in financial services by enabling personalised products and interactions. Responsible AI deployment can improve fairness and reduce bias. The UK's existing regulatory structure offers strong support for oversight without new cross-sectoral legislation. Close coordination between regulators is key to avoid regulatory fragmentation.

The UK's current financial regulatory framework provides a solid foundation for the responsible use of AI, with no need for AI-specific legislation at this time. Emphasising a principles-based, sector-led approach, the UK can balance innovation with risk oversight. Regulatory interoperability with global markets is essential to prevent fragmentation, and any future rules should remain technology-agnostic and proportionate.

How is AI currently used in different sectors of financial services and how is this likely to change over the next ten years?

AI is already in widespread use across financial services, and this trend continues to accelerate. The Financial Conduct Authority (FCA) and Bank of England's 2024 survey on AI and machine learning in UK financial services found that 75% of firms are already using AI, with an

additional 10% planning to adopt it within the next three years[1]. As AI adoption deepens, issues around regulation, ethics, security, transparency, and privacy are expected to become more prominent.

Over the next decade, AI is expected to evolve from a set of experimental tools to a core component of financial services. Firms are currently building strong data infrastructures and testing large language models (LLMs) in controlled public cloud environments. As these models move into production, AI will become integral to services such as personalised financial advice and real-time fraud prevention.

An enabler of this transition is the need for secure, low-latency data processing. Colocation play a role by offering secure, high-bandwidth facilities that allow financial institutions to place their AI infrastructure close to their data. This proximity is important for latency-sensitive applications such as fraud detection and algorithmic trading.

UK financial services firms view AI as a positive force, recognising its potential to increase operational efficiency and enhance customer experience. AI is projected to contribute £35 billion in value to financial and professional business services by 2030, with £2.6 billion in asset management, £0.6 billion in challenger banks, £2.4 billion in fintech, £9.0 billion in insurance, £1.3 billion in investment banking, £9.3 billion in legal services, and £9.9 billion in retail banking[2].

Currently, the majority of AI use cases are concentrated in back-office functions. Natural language processing (NLP) models are widely used for error and fraud detection, identifying anomalies and unusual behaviour such as large transactions from unexpected locations. AI is also increasingly used for process automation, a trend highlighted in the FCA and Bank of England's 2024 survey, which found that 55% of AI use cases involve some level of automated decision-making—24% semi-autonomous and 2% fully autonomous[3]. AI-driven automation is also improving customer service through chatbots and virtual assistants that resolve queries in real time.

Looking ahead, AI is expected to expand into front-office functions over the next decade. This includes customer service, where AI-powered chatbots and assistants will handle complex queries with accurate, verifiable responses, reducing risks such as hallucinations or deceptive outputs. AI will also play a greater role in sales and marketing, enabling personalised campaigns, predictive analytics, and return-on-investment (ROI) measurement. Beyond business processes, financial services employees will increasingly rely on AI as a "digital colleague" to support tasks like ideation, market research, and analysis.

In the technology function of financial institutions, AI will significantly boost productivity in development, testing, and support of financial services applications. It will also accelerate the modernisation of legacy systems, delivering improved cost-to-income ratios and faster time-to-market through AI-driven smart engineering over the next 5 to 10 years.

Emerging AI use cases are also beginning to reshape financial services. Shallowfake detection—targeting manipulated media without relying on deep learning—will be vital for security and fraud prevention. Meanwhile, agentive AI systems, which automate complex

[1] FCA & Bank of England (2024). Survey of AI and machine learning in UK financial services
[2] Frontier Economics (2022). The impact of artificial intelligence on the UK economy.
[3] FCA & Bank of England (2024). Survey of AI and machine learning in UK financial services.

workflows and support user decision-making, are set to enhance operational efficiency and innovation.

Within specific sectors, the banking industry is seeing rapid adoption of AI technologies, including generative AI, banking-specific LLMs, AI-augmented development tools, and "machine customers"—autonomous agents that directly interact with banking systems. The sector is also moving towards intelligent applications that automate tasks, offer personalised recommendations, and enhance user experience.

Regulatory authorities are increasingly adopting AI, particularly in supervisory technology (SupTech). The Financial Stability Board (FSB) reported that 59% of supervisory authorities used AI in 2023, up from 54% in 2022[4]. Key developments include faster economic indicators, use of alternative data in supervisory assessments, and experimentation with LLMs for research, statistical analysis, and document drafting.

Over the next decade, a hybrid AI architecture is expected to emerge. Financial institutions will continue to use the public cloud for development and training, while deploying production-ready models in on-premises data centres or colocation sites. This approach balances cloud scalability with the privacy, performance, and cost-efficiency advantages of local infrastructure.

One notable exception to cloud testing is among large algorithmic trading firms, which are building private GPU research clusters to support AI-driven models. These firms prioritise privacy and cost-effectiveness, and as cluster size—and energy demand—has grown, they have relocated infrastructure to northern Europe (e.g. Norway and Finland) where energy and cooling costs are lower. For instance, XTX Markets has publicly referenced operating a research cluster with 25,000 top-end GPUs[5].

By the end of the decade, AI will have permeated all aspects of financial services—from personalised client experiences to advanced risk management systems.

To what extent can AI improve productivity in financial services?

AI has the potential to significantly enhance productivity across financial services, delivering benefits for institutions, regulators, and consumers alike. Initial impacts may be most evident in advisory firms supporting banks, particularly in data-heavy roles such as reporting, collation, and initial analysis.

AI enhances efficiency by automating routine tasks including data entry, transaction processing, and customer service through virtual assistants, freeing up time and reducing costs. It strengthens fraud detection by analysing vast datasets in real-time to flag suspicious transactions. In risk management, AI models can anticipate market movements and identify vulnerabilities based on historical data and trend analysis, enabling more informed decision-making.

[4] Financial Stability Board (2024). Artificial Intelligence and Machine Learning in Financial Services.
[5] XTX Markets (2024). Public statements on AI infrastructure.

The benefits extend to personalisation and customer experience. AI enables the development of tailored financial products based on individual behaviours and preferences. Robo-advisors provide customers with bespoke financial advice and investment strategies, improving financial health and accessibility. Furthermore, AI-powered chatbots offer 24/7 support, improving convenience and customer satisfaction.

From a regulatory standpoint, AI supports compliance by monitoring transactions, flagging anomalies, and streamlining reporting. Supervisory bodies can use AI for market surveillance, economic monitoring, and data analysis to identify systemic risks and trends. The technology also contributes to the development of better financial products and services, helping consumers make informed decisions and enhancing overall financial security.

Despite its promise, AI adoption in financial services faces several barriers. A major challenge is the quality and completeness of input data, which can limit the effectiveness of AI models. Institutions may also lack clarity about appropriate use cases and desired outcomes, further complicated by uncertainty around regulatory expectations. The risk-averse culture of financial institutions exacerbates this hesitation, particularly where AI applications are not yet fully understood.

Legacy infrastructure is a significant hurdle. Many financial institutions, regardless of size, operate on outdated systems that are incompatible with modern AI applications. Updating or replacing these systems often requires substantial investment. In parallel, upskilling employees remains essential to support the integration and responsible use of AI.

However, financial services firms are generally well-positioned to adopt AI within existing governance and risk frameworks. Traditional machine learning and predictive models are already deployed safely and effectively. Generative AI (GenAI) can build upon this foundation, particularly when integrated through secure hyperscale cloud platforms, which make scalable AI solutions accessible even to smaller enterprises.

Hardware availability is another constraint. The pace of innovation in GPU technology—the core enabler of AI applications—has made it difficult for individual firms to keep up. Hardware can become outdated shortly after procurement, making firms increasingly reliant on hyperscalers to access the latest GPUs for development and testing. The recent US AI Diffusion Rule, which restricts exports of key AI components, currently exempts the UK due to its Tier 1 status. However, these restrictions may encourage alternative innovation in other regions, indirectly reshaping the global supply chain.

Deploying AI at scale also presents infrastructure challenges. Advanced AI workloads demand specialised facilities with high energy capacity and liquid cooling systems, which many legacy data centres lack. Upgrading these sites is expensive and complex. In a tightening energy landscape, securing adequate power supply adds an additional layer of difficulty.

Colocation providers can support AI deployment. Their purpose-built facilities support high-density workloads with advanced systems, robust power infrastructure and long-term renewable energy contracts. By utilising these, financial institutions can avoid major capital outlays for retrofitting, helping to accelerate AI adoption.

In addition, AI-as-a-service offerings—such as those from NVIDIA—present another pathway. These services, deployed within secure colocation environments, provide access to private AI infrastructure with dedicated resources and enhanced security. This is particularly beneficial

for institutions subject to stringent data governance requirements. While public cloud solutions can also lower barriers to entry, they may fall short of meeting regulatory and internal security standards. A hybrid approach, blending the scalability of public cloud with the control of private deployments, offers a practical solution for firms balancing innovation, compliance, and performance.

In the context of GenAI, financial institutions must approach implementation with careful risk assessment, mitigation, and monitoring. While GenAI offers significant potential to enhance productivity and customer interaction, the sector's sensitivity demands that use cases be evaluated rigorously to ensure alignment with regulatory expectations and ethical standards.

The UK financial services sector is well-positioned globally to capitalise on AI. It benefits from a strong talent pool, a pragmatic and innovation-friendly regulatory environment, and a globally respected legal framework. Compared to the EU, the UK offers more flexibility in AI experimentation and deployment. With strategic collaboration, the UK could act as a gateway for AI into Europe. That said, global competition is fierce, and more permissive or better-incentivised markets may attract talent and investment elsewhere. Infrastructure readiness—particularly around AI-capable data centres—will be critical to maintaining leadership in this space.

As AI transforms workflows, demand for AI-related skills is growing rapidly. This presents an opportunity for workers across disciplines to adapt and grow. Upskilling empowers employees to engage confidently with emerging technologies, overcoming apprehension and unlocking creativity. Done well, AI can democratise access to opportunities, reduce the burden of rote tasks, and enable professionals to focus on higher-value, human-centric work.

What are the risks to financial stability arising from AI and how can they be mitigated?

While AI does not inherently pose unique risks to financial stability, its application across the financial sector introduces new challenges that will be carefully assessed, monitored, and managed by industry.

AI can help to address the risk relating to cyber security. Injection attacks, for instance, pose an escalating threat to financial services. AI systems are often the most effective tools for detecting and responding to such intrusions. In the United States, the Federal Trade Commission's Consumer Sentinel Network recorded a 45% increase in identity theft in early 2024, with aggregate fraud losses surpassing $10.2 billion[6]. Imposter scams alone accounted for nearly $2.7 billion in losses, underscoring a rapid rise in financial crime. In addition, synthetic media attacks have emerged as a recognized and growing form of financial fraud.

AI-enabled biometric verification solutions are increasingly critical in countering these threats. These tools, aligned with the European Banking Authority's Good Practice Guide[7], represent the most effective approach for Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance. Injection attack detection has been available for several years, but as the capabilities of malicious actors evolve, even well-trained human examiners now struggle to detect sophisticated face swap attacks. AI is not only a valuable tool—but a necessary one.

[6] U.S. Federal Trade Commission, Consumer Sentinel Network Data Book (2024)

[7] European Banking Authority, "EBA Report on Good Practices on the Use of AML/CFT Biometrics", March 2023

AIFS0059

Some members of techUK have expressed concerns that the UK banking sector is falling behind global peers in adopting these critical technologies.

Cybersecurity and digital operational resilience are fundamental to maintaining market stability. The UK's financial system is underpinned by data centres and network infrastructure, which support essential functions ranging from online banking and payment processing to algorithmic trading and risk modelling. Disruptions to these systems could trigger instability and erode public trust. As such, the resilience and security of this infrastructure are vital.

To address this, the Financial Conduct Authority (FCA) and UK government have implemented robust operational resilience and cybersecurity regulations. These frameworks require financial institutions to identify critical business services, define impact tolerances, and conduct regular scenario testing to ensure continuity during cyberattacks, natural disasters, or technological failures[8]. These measures are designed to ensure that essential services remain operational during times of disruption.

The UK government has also recently designated data centres as part of the nation's Critical National Infrastructure (CNI), recognizing their central role in supporting the economy. This classification places them alongside essential services like energy and water, enabling the government to offer enhanced support during crises and to aid in long-term recovery and planning[9].

The complexity of AI models also introduces unique risks, particularly when it comes to third-party dependencies and embedded or 'hidden' models. Financial institutions often rely on AI tools provided by external vendors, which may limit transparency into how models function and evolve. This reliance increases the importance of strong AI governance frameworks. In the United States, The National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF) provides one such approach, offering practical guidance to organizations on how to map, measure, manage, and govern AI risk[10]. Developed through a transparent, consensus-based process involving public and private sector input, the NIST AI RMF is a flexible and actionable resource that can support financial institutions in implementing responsible AI practices aligned with their specific risk profiles and regulatory obligations.

Other emerging AI-related risks include hallucinations in generative AI models and herding behaviour in markets. Hallucinations—where models generate false or misleading outputs—could be particularly damaging in high-stakes financial decision-making or automated reporting. Likewise, the use of AI trading algorithms informed by social media content introduces new volatility risks. Overreliance on similar sources or models can exacerbate herd behaviour, potentially amplifying market movements in ways that traditional oversight mechanisms may struggle to contain.

While concerns are sometimes raised about AI market concentration, it is important to note that the AI ecosystem is currently broad and diverse. More than 50 significant providers operate across the landscape, and the number is growing[11]. This diffusion reduces the risk of over-

[8] FCA Policy Statement PS21/3 – Building Operational Resilience, March 2021
[9] UK Government designation of data centres as Critical National Infrastructure, Cabinet Office, 2024
[10] National Institute of Standards and Technology (NIST), "AI Risk Management Framework", January 2023.
[11] Industry analysis compiled from Gartner and McKinsey reports, 2024

reliance on a small group of dominant vendors. However, continued monitoring is essential to ensure a competitive, resilient, and transparent AI market.

In summary, AI presents both new opportunities for the financial sector. With appropriate governance, robust infrastructure, and ongoing regulatory engagement, any potential risks can be effectively mitigated to safeguard financial stability.

What are the benefits and risks to consumers arising from AI, particularly for vulnerable consumers?

AI has the potential to significantly transform financial services, offering considerable benefits to consumers through the processing of vast datasets and the increased personalisation of products, services, and interactions. When supported by an enabling regulatory environment, AI can help firms tailor support more effectively, particularly for vulnerable consumers, ensuring they receive appropriate and timely assistance.

Many financial services firms are already custodians of extensive consumer datasets. AI technologies can help unlock the value of this data, not only to improve customer outcomes but also to develop innovative products and new business streams. Capabilities such as conversational interfaces ("talk to data") and automated insight generation can support more informed decision-making around capital allocation and risk management.

When designed and deployed responsibly, AI systems—especially non-autonomous ones—do not inherently increase the risk of embedding bias in decision-making. These systems reflect the data and rules they are given. Therefore, with diverse and representative training data, appropriate weighting, and ongoing monitoring, AI can actually bias compared to human decision-making. In this sense, AI offers an opportunity to improve fairness and consistency in financial services delivery.

To realise these benefits, it is vital that the UK government continues with the principles-based regulatory approach set out in the 2023 AI White Paper[12]. This framework provides industry with the certainty needed to develop AI-enabled products, whether they fully rely on AI or use it in specific components. The Information Commissioner's Office (ICO), Financial Conduct Authority (FCA), and Competition and Markets Authority (CMA) have all expressed support for this approach in their strategic updates, affirming that no new cross-sectoral AI-specific legislation is currently required. techUK shares this view and cautions that premature regulation could stifle innovation, placing unnecessary burdens on UK-based AI developers before the sector has had the opportunity to demonstrate its broader societal value.

Importantly, the AI principles should not be viewed in isolation. They are part of a wider ecosystem of consumer protection, sitting alongside existing legal and regulatory frameworks such as the Equality Act 2010 and the UK General Data Protection Regulation. These established protections continue to apply and will guide responsible AI deployment.

[12] UK Government, *A Pro-Innovation Approach to AI Regulation: Government White Paper*, March 2023.

While existing financial services regulations provide robust oversight—particularly around risk and third-party outsourcing—there may be a case in future for targeted legislative updates if clear gaps are identified. However, at present, adapting existing frameworks with clarity and avoiding overly prescriptive, technology-specific rules remains the most pragmatic and future-proofed approach.

Data privacy must remain at the heart of AI deployment in financial services. Firms must comply with relevant data protection laws and maintain transparency around how data is collected, stored, and used. Innovations such as differential privacy and advanced encryption methods provide practical solutions that help protect sensitive data while still enabling meaningful innovation.

Firms operating in the sector are already subject to oversight by regulators such as the FCA and the ICO. The AI principles should therefore be viewed as an additional, complementary layer of guidance—further strengthening protections rather than introducing redundancy or conflict.

Robust governance frameworks are essential to ensure AI systems remain safe, fair, and effective over time. Models must be continuously monitored for performance drift or degradation, and evaluation protocols—such as testing against large, real-world datasets or historical decision-making outcomes—should be standard practice. Shadow testing, where an updated system runs in parallel with an existing one without making live decisions, can also help organisations identify and correct emerging issues before real-world deployment. Independent audits or third-party attestations can further reinforce trust, particularly where bias mitigation is a concern.

As the UK seeks to unlock the full potential of AI in financial services, it is critical that sectoral regulators coordinate closely through bodies such as the Digital Regulation Cooperation Forum (DRCF). Avoiding fragmented or competing regulatory requirements will be essential to fostering innovation, ensuring consistency, and delivering clear guidance to firms and consumers alike.

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?

Current financial services regulation provides a strong foundation for the safe and responsible use of AI. We support the FCA's recent statement affirming that new AI-specific regulations are not necessary at this time, and that existing frameworks can sufficiently govern AI development without stifling innovation. We also endorse the Government's approach as set out in the AI White Paper (2023), which promotes agile, sector-led regulation. By placing oversight responsibilities with existing regulators, who understand the unique needs and risks of their respective sectors, the framework remains adaptable and fit-for-purpose as technology evolves.

In a global context, it is essential that the UK avoids developing AI regulations in isolation. Ensuring interoperability with other jurisdictions is critical to prevent market fragmentation,

regulatory misalignment, and the duplication of compliance burdens for firms operating internationally. Prescriptive regulation that deviates from a risk-based, principles-driven approach could hinder innovation, particularly for firms operating at global scale — whether financial institutions or technology providers. Regulatory cooperation across borders will be key to unlocking AI's full potential, enhancing productivity, operational resilience, and risk management at scale.

To support innovation while providing regulatory clarity, industry-facing tools and services are vital. We strongly support initiatives such as the FCA's Innovation Pathway, which offers tailored guidance to help firms navigate evolving regulatory requirements. As demand for clarity around AI-related authorisations grows, such services will play a crucial role in fostering innovation and compliance in financial services.

Any future regulation should remain technology-agnostic, principles-based, and proportionate to risk. Over-regulation may result in unintended consequences, such as deterring smaller firms or new entrants from adopting AI and realising its potential for innovation and productivity gains.

The financial sector already benefits from a suite of regulatory guidance, including the EBA's outsourcing recommendations, the UK PRA's Supervisory Statement SS2/215, and recent updates from the Financial Stability Board (FSB) and Bank for International Settlements (BIS), which address outsourcing and cloud risks. However, further clarity is needed to ensure consistent and confident application of these frameworks in the AI context. Key areas where guidance is required include:

- UK GDPR Application: While the ICO's recent guidance on generative AI and data protection highlights transparency and accountability requirements, firms would benefit from more practical direction—particularly regarding emerging uses such as agentic AI.
- Senior Managers and Consumer Duty: Clarification is needed on expectations under the Senior Managers and Certification Regime and how Consumer Duty applies when AI is embedded in service delivery or decision-making processes.
- Cybersecurity Standards: As AI adoption accelerates, institutions must invest in enhanced cyber infrastructure. A minimum cybersecurity threshold for AI use is necessary to mitigate evolving threats. Given the international nature of AI development and supply chains, the UK should champion global AI cybersecurity standards to ensure consistency and prevent fragmented approaches. Standardisation in this area is critical to maintaining security, resilience, and trust in AI systems.
- Use Case-Specific Risks: Further analysis is needed on AI's impact across various financial sub-sectors, including:
    - AI-powered trading bots and their potential effect on market dynamics;
    - Competitive advantages leveraged through AI in wealth management, with potential to widen inequality;
    - The governance and accountability challenges posed by Robo-Advisors and the provision of potentially poor financial advice;
    - Safeguards needed to protect fintech innovation and consumer services.

AIFS0059

Governance mechanisms must be in place to monitor AI system use, assess their risk levels, and evaluate market impacts. According to a recent Bank of England (BoE) survey[13], AI adoption in financial services has risen sharply, with 75% of firms now using the technology—up from 53% two years ago. Over half of current use cases involve some degree of automated decision-making. We welcome initiatives like the BoE's AI consortium, which brings together private sector expertise to better understand risks. However, to ensure fresh and diverse thinking, this expertise must come from both within and outside the financial sector.

As AI adoption deepens, the UK must also consider how to retain its trade advantage in financial services. This includes strategies to keep more data onshore, improve data privacy and governance practices, and reinforce trust in responsible data use. Supporting data infrastructure, including investment in data centres, will be critical to enabling sustainable AI growth.

The UK is well-positioned to lead in the responsible development of AI, thanks to its deep pool of financial and technical expertise, an internationally respected legal system, and a proportionate regulatory regime—particularly when compared with the EU. With the right balance of innovation support and consumer protection, the UK could position itself as a gateway for AI-driven financial services across Europe. However, ongoing vigilance is essential to ensure that more permissive environments elsewhere do not divert investment and talent. Supporting legal and regulatory expertise in AI will also be key to realising this opportunity.

April 2025

[13] https://www.bankofengland.co.uk/report/2024/artificial-intelligence-in-uk-financial-services-2024#:~:text=75%25%20of%20firms%20are%20already,58%25%20and%2014%25%20respectively.