A Response to AI in Financial Services Inquiry
11 April 2025

Executive summary:

In response to this call for evidence on AI in Financial Services by the Treasury Committee of the UK Parliament, I provide evidence and policy recommendations to the following questions from the terms of reference:

- What are the risks to financial stability arising from AI and how can they be mitigated?
- What are the benefits and risks to consumers arising from AI, particularly for vulnerable consumers?

I call for the following policy recommendations:

- HM Treasury and Financial Conduct Authority (FCA) should expand existing market abuse regulations to explicitly include AI-driven manipulations. These regulations should include severe penalties for violations and require companies to clearly label AI-generated content.

- HM Treasury and the FCA should develop technology to monitor algorithmic trading in real-time. This technology would automatically detect and block transactions if they violate rules.

- HMG should work with other governments and financial watchdogs to establish global AI governance standards to prevent cross-border instability, designate AI infrastructure providers as critical financial market participants, and subject them to periodic stress testing.

- HMG should mandate explainability in AI systems making critical financial decisions and conduct regular bias audits. Financial services providers should be required to operate a hybrid service model with human support to assist vulnerable consumers.

Response author:

PK Senyo is a Professor of FinTech and Information Systems and the Associate Dean for Research at Southampton Business School, University of Southampton. PK's research focuses on how emerging technologies such as AI, digital platforms, and FinTech shape the transformation, provision, and effective delivery of digital services with broader implications for individuals, organisations, and society.

PK's research has been published in leading journals such as the *Information Systems Journal, European Journal of Information Systems, Journal of Strategic Information Systems*, and *British Journal of Management*, among others. He has obtained over £1 million in research income from councils and through consultancy for private and public sector organisations. PK regularly consults and provides expert advice on digital technology projects for national and international organisations. He has previously consulted for the UK Government, the World Bank, and the International Telecommunication Union (ITU).

RESPONSE:

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

Like any emerging digital technology, AI is a double-edged sword that has inherent benefits and risks. AI's emergence poses increased risks to cybersecurity for the following reasons. With AI, more sophisticated cyber-attacks can be launched with minimal effort, resources, and experience due to the capabilities it offers (Ostmann & Dorobantu, 2021). Given that most AI models are trained on existing

data, this practice increases cybersecurity risks because these training data could be manipulated to introduce vulnerabilities and reverse-engineer AI models to bypass security protocols, leading to inaccurate financial decisions. More importantly, the over-reliance on AI for cybersecurity increases the risks of automation bias and false positives and negatives, leading to the misclassification of threats and failure to detect sophisticated cyberattacks.

I believe the first risk to financial stability from AI is cybersecurity risks, including AI-driven attacks, as well as data privacy and breaches (Ostmann & Dorobantu, 2021). Advancements in AI have provided technology tools and computing resources to automate large-scale cyber-attacks through deepfakes, malware, and phishing. The second risk is the shift toward algorithm trading, which relies largely on social media sentiments, which makes it susceptible to market manipulation and amplification of false signals (Ciciretti et al., 2025). When AI models misinterpret social media sentiments and are unable to detect coordinated social media campaigns, they may authorise wrong trades, leading to financial instability (Daníelsson et al., 2022). Third, there are risks associated with generative AI hallucination in terms of falsifying financial information and stock performance, as well as market volatility due to algorithm deadlock. Lastly, there is a risk of overreliance on a few large technology solution providers, creating a single point of failure risk.

The following corresponding mitigation strategies are proposed:

1- First, traditional financial security measures and tools need to be revamped to include technologies for detecting and automatically thwarting AI-driven cyber-attacks. The implementation of these tools should be backed by frameworks that promote AI transparency in cyber security as well as cross-industry intelligence sharing on AI-based cybersecurity threats (Ostmann & Dorobantu, 2021).

2- Second, explainable AI should be promoted to improve the transparency of algorithmic trading, coupled with periodic auditing of financial AI algorithms to proactively detect and address emerging threats.

3- Third, there is a need to build human oversight into AI decision-making to serve as circuit-breakers (Buckley et al., 2021) in trading systems to prevent market distortion and verify contents to detect false signals.

4- Lastly, there should be increased regulatory oversight on providers of AI services to ensure compliance and implementation of continency and disaster recovery plans.

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

AI offers many benefits to customers, such as improved access to financial services, personalised financial advice and support, fraud detection, and customer protection (Gomber et al., 2018).

1- For instance, with a simple prompt, customers could get information on many financial services, compare different services, and make more informed decisions. More importantly, AI tools have accessibility features such as voice assistance and screen readers for vulnerable customers.

2- Relatedly, AI could enable the use of alternative data, such as mobile phone usage and social media data to extend banking and credit to financially excluded individuals. These benefits significantly increase and improve access to financial services for many individuals, especially vulnerable citizens.

3- In addition, AI can provide personalised financial advice and support to customers in real-time without human intervention. For instance, AI can provide insights into spending habits and

suggest appropriate mitigation actions to ensure financial discipline. With the rise of "elder fraud" and cryptocurrency fraud in the UK, AI can monitor, provide real-time alerts, and block suspicious financial transactions, providing another layer of protection to vulnerable customers.

On the other hand, AI also poses significant risks to customers, especially vulnerable people, through algorithmic bias and discrimination, privacy and data misuse risks, digital exclusion, AI-powered scams, and dynamic pricing and exploitation (Daníelsson et al., 2022).

1- AI models trained on biased data could use this to discriminate against vulnerable individuals such as minorities, women, and elderly people. For instance, if AI models that generate insurance prices are trained on data that discriminate based on demographic characteristics, this could result in exploitation and increased pricing for vulnerable people.

2- Because of the vast amount of data AI models use, it increases the exposure to breaches and misuse since customer data collected specifically to provide innovative services can be used in other related projects. For instance, alternative data collected on a customer such as mobile phone usage, intended to provide increased financial services could be easily analysed to know their daily patterns, leading to privacy breaches.

3- Given that AI systems require a smartphone and some digital skills to operate, many vulnerable people, such as elderly and low-income individuals may be digitally excluded. For instance, the shift to app-only banking and the use of AI chatbots in financial services reduces access for vulnerable people and poses a risk of exclusion.

4- While AI can be used to prevent cyber fraud, it equally has the potential to spearhead large-scale fraud. AI can be used to easily create deepfakes, phishing bots, viruses, and stage multiple cyber-attacks with minimal cybersecurity expertise and resources. AI tools have been used in the past for impersonation, leading to wire transfer fraud. For vulnerable individuals who are most often not digitally savvy and unable to quickly detect AI-generated content, AI increases their susceptibility to AI-powered scams.

References:

Buckley, R. P., Zetzsche, D. A., Arnert, D. W., & Tang, B. W. (2021). Regulating Artificial Intelligence in Finance: Putting the Human in the Loop. *Sydney Law Review*, *1*(43), 43–82. http://orcid.org/0000-0002-6910-7311.

Ciciretti, V., Nandy, M., Pallotta, A., Lodh, S., Senyo, P. K., & Kartasova, J. (2025). An early-warning risk signals framework to capture systematic risk in financial markets. *Quantitative Finance*.

Daníelsson, J., Macrae, R., & Uthemann, A. (2022). Artificial intelligence and systemic risk. *Journal of Banking and Finance*, *140*. https://doi.org/10.1016/j.jbankfin.2021.106290

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services. *Journal of Management Information Systems*, *35*(1), 220–265. https://doi.org/10.1080/07421222.2018.1440766

Ostmann, F., & Dorobantu, C. (2021). *AI in Financial Services*. https://doi.org/doi.org/10.5281/zenodo.4916041

https://doi.org/10.5258/SOTON/PP0128