# Financial institutions race to master AI amid rising adversarial threats



The financial services sector, long known for its early adoption of technological advancements, is currently experiencing a significant shift as it embraces artificial intelligence (AI) at an unprecedented rate. According to a recent survey by the Bank of England and the Financial Conduct Authority, 75% of financial institutions are already employing AI technologies, with an additional 10% planning to implement AI within the next three years. This swift integration opens up vast opportunities, ranging from improved fraud detection to enhanced analytics capabilities. However, it also introduces a myriad of complexities that organisations must navigate carefully.

Despite the apparent advantages, the reality is that many financial firms do not fully grasp the intricacies of AI technology. The survey indicates that only about a third of these institutions feel confident in their understanding of how AI operates. Given the rapid advancement and potential malicious use of AI, financial institutions must deepen their comprehension of the technology. This is especially crucial as adversarial AI—where attackers manipulate algorithms and data inputs—poses significant threats. Such vulnerabilities could lead to manipulated market forecasts or undetected fraudulent transactions, presenting challenges that traditional cybersecurity measures cannot address.

The increasing prevalence of adversarial AI calls for a paradigm shift in how financial institutions approach security. For instance, regulators and companies alike are becoming more attuned to concepts like data poisoning and inference-time attacks. Initiatives are underway to ensure that regulatory frameworks evolve in tandem with technological advancements. The Bank of England, under the leadership of Sarah Breeden, has indicated its commitment to understanding these risks. She noted the importance of integrating AI into stress tests to better understand the potential implications on market stability.

AI's influence extends beyond merely operational improvements; it brings inherent risks that demand vigilance from financial managers. U.S. Treasury Secretary Janet Yellen has articulated these concerns, highlighting that while AI can lower transaction costs and enhance efficiency, it also brings complexities that could lead to significant vulnerabilities. For example, the reliance on similar data and models across multiple participants increases the systemic risk, especially during market stresses. Yellen advocates for a coordinated approach among regulators to mitigate these risks, emphasising the need for scenario analysis to anticipate and address potential challenges.

Regulatory bodies, including the European Securities and Markets Authority (ESMA), are also responding proactively. ESMA's recent guidelines assert that banks and investment firms must maintain accountability for decisions made by AI tools, necessitating a sound understanding of AI within management. The regulatory landscape is increasingly focused on protecting clients, particularly retail investors, amid growing concerns over the misuse of AI technology. Compliance with established frameworks, such as the MiFID securities law, is essential, ensuring that firms employ AI responsibly while still harnessing its capabilities to enhance service delivery and risk management.

As AI continues to integrate into various aspects of financial operations—ranging from customer service to cyber defence—its potential to reshape traditional roles cannot be overlooked. Experts suggest that while some jobs may diminish, new positions are likely to emerge, such as AI ethicists and transaction monitors. The emphasis on enhancing operational resilience through AI adoption also indicates a shift towards a more innovative financial landscape.

In light of these developments, there is an urgent need for financial institutions to arm themselves with enhanced knowledge and robust training programmes concerning AI and its associated risks. A well-structured approach to risk management will not only help in leveraging AI to its fullest potential but also ensure that firms are prepared to defend against the distinct threats posed by adversarial AI. With regulatory frameworks evolving and greater scrutiny placed upon AI use, financial services must prioritize security, governance, and ethical considerations as they navigate this transformative era.

AI has firmly established its foothold in the financial services sector; now is the time for institutions to fortify their understanding and management of this powerful technology. The journey towards secure, responsible AI integration is not merely a technological upgrade but a vital evolution to safeguard the interests of both financial institutions and their customers.

## Reference Map:

* Paragraph 1 – [[1]](https://www.theregister.com/2025/05/29/qa_adversarial_ai_financial_services_2025/), [[2]](https://www.ft.com/content/d4d212a8-c63a-4b00-9f4c-e06ed59f9279), [[4]](https://www.ft.com/content/9ffe888e-2f78-4f59-9536-2e31f5bde8b7)
* Paragraph 2 – [[1]](https://www.theregister.com/2025/05/29/qa_adversarial_ai_financial_services_2025/), [[2]](https://www.ft.com/content/d4d212a8-c63a-4b00-9f4c-e06ed59f9279), [[3]](https://www.reuters.com/business/finance/yellen-warn-significant-risks-use-ai-finance-2024-06-05/)
* Paragraph 3 – [[3]](https://www.reuters.com/business/finance/yellen-warn-significant-risks-use-ai-finance-2024-06-05/), [[5]](https://www.reuters.com/business/finance/eu-watchdog-says-banks-must-take-full-responsibility-when-using-ai-2024-05-30/)
* Paragraph 4 – [[2]](https://www.ft.com/content/d4d212a8-c63a-4b00-9f4c-e06ed59f9279), [[5]](https://www.reuters.com/business/finance/eu-watchdog-says-banks-must-take-full-responsibility-when-using-ai-2024-05-30/)
* Paragraph 5 – [[4]](https://www.ft.com/content/9ffe888e-2f78-4f59-9536-2e31f5bde8b7)
* Paragraph 6 – [[1]](https://www.theregister.com/2025/05/29/qa_adversarial_ai_financial_services_2025/), [[6]](https://www.bankofengland.co.uk/financial-stability-in-focus/2025/april-2025)
* Paragraph 7 – [[7]](https://timlaytonllc.com/2025/03/27/adversarial-ai-threats-in-financial-services-a-zero-trust-approach-to-defense/)
* Paragraph 8 – [[1]](https://www.theregister.com/2025/05/29/qa_adversarial_ai_financial_services_2025/)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.theregister.com/2025/05/29/qa_adversarial_ai_financial_services_2025/> - Please view link - unable to able to access data
2. <https://www.ft.com/content/d4d212a8-c63a-4b00-9f4c-e06ed59f9279> - In a recent discussion, Sarah Breeden, Deputy Governor of the Bank of England, highlighted the rapid adoption of generative artificial intelligence (AI) within the financial sector, noting that 75% of companies are now utilising AI. This swift integration introduces potential risks, including sophisticated market manipulation and increased volatility during stress periods. To address these challenges, the Bank of England is considering incorporating AI into its annual stress tests and has established an 'AI consortium' with private sector experts to further study these risks. Breeden emphasised the necessity for financial managers to comprehend and manage AI models, which often operate autonomously, to mitigate associated risks.
3. <https://www.reuters.com/business/finance/yellen-warn-significant-risks-use-ai-finance-2024-06-05/> - U.S. Treasury Secretary Janet Yellen is set to address the significant risks associated with the use of artificial intelligence (AI) in the financial sector during a speech at a Financial Stability Oversight Council and Brookings Institution AI conference. While acknowledging that AI can reduce transaction costs, Yellen points out vulnerabilities due to the complexity and opacity of AI models, inadequate risk management, and the reliance on similar data and models by many market participants. She also highlights risks from vendor concentration and potential biases from insufficient or faulty data. Despite these challenges, Yellen recognises the benefits of AI in automating customer support, improving efficiency, and enhancing fraud detection. The Treasury Department is collaborating with financial regulators to mitigate illicit finance risks using AI and emphasises the need for scenario analysis to understand emerging risks and opportunities. The Financial Stability Oversight Council will continue monitoring AI's impact and promoting dialogue among regulators to enhance financial stability.
4. <https://www.ft.com/content/9ffe888e-2f78-4f59-9536-2e31f5bde8b7> - The financial services sector is increasingly leveraging artificial intelligence (AI) to boost productivity and innovation. AI is being implemented in various areas, such as customer support, underwriting, pricing, cyber defence, and crime detection. Experts in the field, like Peter Weston from Harvey Nash and Michael Conway from IBM Consulting, note that the demand for high-end digital experiences and the need to improve operational resilience are major drivers for AI adoption. AI is expected to augment human roles by creating new jobs, including prompt engineers, transaction monitors, and AI ethicists, while some traditional roles, like help desk support and coders, may diminish. Cybersecurity is also poised to benefit from AI technology. Regulatory frameworks, such as those being developed by the UK government, are essential to ensure safe and responsible AI deployment in the industry.
5. <https://www.reuters.com/business/finance/eu-watchdog-says-banks-must-take-full-responsibility-when-using-ai-2024-05-30/> - The European Securities and Markets Authority (ESMA) has declared that banks and investment firms in the EU cannot avoid boardroom responsibility and legal obligations to protect customers when using artificial intelligence (AI). In its first statement on AI, ESMA outlined how financial firms can incorporate AI in their operations without violating the EU's MiFID securities law. While AI has the potential to enhance investment strategies and client services, it also carries significant risks, particularly for retail investor protection. ESMA emphasised that firms' management bodies are responsible for decisions made by AI tools and must prioritise client interests. This responsibility extends to AI technologies developed in-house or acquired from third parties, such as ChatGPT and Google Bard. Firms' management must understand and oversee the use of AI technologies. This guidance is aligned with compliance under MiFID, distinct from upcoming EU AI rules intended to set a global standard for AI in business and daily life. Additionally, global efforts, including those by G7, aim to ensure the safe development of AI technology.
6. <https://www.bankofengland.co.uk/financial-stability-in-focus/2025/april-2025> - The Bank of England is actively integrating artificial intelligence (AI) into its operations to enhance financial stability. AI is being utilised in various areas, including the Bank's Agency network, where a generative AI solution is being developed to support Agents in extracting insights from company visits. Additionally, AI methods are playing a role in analysing regulatory and market data, producing synthetic data, and summarising external reports. To ensure the safe and effective use of AI, the Bank has established policies and a governance framework, guided by seven principles to ensure AI solutions are Targeted, Reliable, and Secure, clearly Understood, supported with Ethical guidance, stress-Tested, and Durable. An Artificial Intelligence and Data Ethics Governance Committee has been set up to oversee the internal use and development of AI solutions, ensuring alignment with these principles.
7. <https://timlaytonllc.com/2025/03/27/adversarial-ai-threats-in-financial-services-a-zero-trust-approach-to-defense/> - Adversarial AI refers to the deliberate manipulation of AI and machine learning systems to produce incorrect, misleading, or malicious outcomes. In the financial industry, these attacks pose serious consequences, including poisoned training data that alters credit scoring algorithms, crafted inputs that evade fraud detection systems, deepfakes and synthetic identities used to bypass KYC and AML checks, and reverse-engineered models that leak proprietary algorithms or decision logic. To defend against these threats, a Zero Trust approach is recommended, which involves strict access controls, continuous verification, micro-segmentation of AI pipelines, enhanced visibility and behaviour analytics, immutable and controlled data sources, and automated incident response. This strategy requires strategic alignment across cybersecurity, data science, risk management, and executive leadership to effectively mitigate adversarial AI threats.