AIFS0051

Written evidence submitted by We Fight Fraud

Summary

This submission, by financial crime prevention consultants We Fight Fraud, provides a practitioner-led, evidence-based examination of the role of Artificial Intelligence (AI) in combating fraud within the UK financial services sector. Drawing on a survey of 150 financial professionals and in-depth interviews with fraud experts and AI providers, the report highlights how AI is transforming fraud detection and prevention—through machine learning, behavioural analytics, network analysis, and natural language processing.

The document outlines current applications, including industry case studies from banks, fintechs, and insurers, and addresses emerging threats such as synthetic identities and deepfake fraud. It also explores the intersection of AI with organisational culture, workforce preparedness, and ethical challenges, calling attention to barriers like legacy systems, skills gaps, and regulatory ambiguity.

Key recommendations include sector-wide AI literacy training, improved data sharing, enhanced regulatory guidance, and support for ethical, people-first AI innovation. The report advocates for a balanced, collaborative approach where AI augments human expertise to build resilience against rapidly evolving financial crime.

Prepared By:

Dr Nicola Harding, CEO WE Fight Fraud

With a PhD in criminology, Dr Harding is an expert in fraud prevention, cybercrime, and financial crime. An advisor to UK Government, her career has been marked by her passion for bridging the gap between academia and industry, using research and technology to design practical solutions to combat fraud. Dr. Harding has worked extensively in academic settings, collaborating with various private and public stakeholders to develop cutting-edge risk mitigation and fraud detection strategies.

Dr Mark Goldspink, Chair, We Fight Fraud

Former CEO at the AI Corporation, now Chair of We fight Fraud, Dr Mark Goldspink has a distinguished career, beginning with a PhD in Chemistry that led to becoming a leader in the oil industry before moving towards his passion of applying AI solutions to solving business problems and driving improvements in fraud and financial crime prevention and detection within the payments sector.

About We Fight Fraud

1. We Fight Fraud is an independent organisation comprising a multidisciplinary team of former senior law enforcement officials, security experts, and academic researchers. Our collective experience spans digital forensics, social engineering, financial crime, serious organised crime, counter terrorism, and regulatory compliance. We work collaboratively across sectors to

identify, understand, and disrupt the mechanisms of fraud and other economic crimes that affect consumers, businesses, and public institutions.

2. Our mission is to protect people and organisations from the real-world impact of fraud by uncovering emerging threats, raising awareness, and informing smarter policy. We do this through intelligence-led research, practical testing, and engagement with regulators, financial institutions, and technology platforms.

3. This research into the future of fraud and Artificial Intelligence includes analysis of a survey completed by 150 financial services staff, including 20% identifying as senior leadership (Head of Fraud, Money Laundering Regulatory Officer (MLRO) or similar), and 25% as fraud intelligence analysts/ investigators. The remaining 55% represented all other areas of financial services, with between 3-15years plus experience working in the sector. This is supplemented with in-depth, anonymous, interviews with Heads of Fraud from three UK Financial institutions and two Subject Matter Experts from AI Technology providers.

4. Our investigation aims to provide policy makers with an evidence-based, practitioner-led perspective on the role of Artificial Intelligence in the future of fraud prevention and detection in financial services, covering not only the current and historical use, but also the relationship between its use and corporate cultures within financial services.

5. We submit this report in the public interest, with the aim of supporting a more informed debate on how Artificial Intelligence can best be used in financial services to combat the threat of financial crime.

About AI use for fraud prevention and detection in Financial Services

6. Financial fraud and money laundering are pervasive threats, accounting for a large share of crime and losses. In the UK, fraud now makes up 36% of all crime (3.2 million incidents in the year to March 2024)[1]. Financial institutions are responding by increasingly deploying artificial intelligence (AI) to detect and prevent fraudulent activities.

7. A recent Bank of England/FCA survey found that 75% of UK financial firms were using AI in 2024 (up from 58% in 2022), with fraud detection cited as one of the top use cases (33% of firms) alongside process optimisation and cybersecurity[2].

8. AI techniques are now embedded in many fraud prevention systems, augmenting or replacing traditional rule-based controls. Key technologies and methods include:

8.1 *Machine Learning Models (Supervised & Unsupervised)*
The primary use of AI in fraud defence today is through machine learning models that flag transactions, behaviours, or content outside the norm[3]. Supervised learning (e.g. decision trees, random forests, gradient boosting, neural networks) is trained on labelled fraud examples to recognise known fraud patterns. Unsupervised and anomaly detection methods (e.g. clustering algorithms, autoencoders, Isolation Forest) identify outliers without prior labels,

[1] https://www.fca.org.uk/news/speeches/frameworks-effective-fraud-prevention-measures
[2] https://www.globalfinregblog.com/2024/11/regulators-publish-third-uk-financial-services-artificial-intelligence-survey
[3] https://www.pwc.co.uk/forensic-services/assets/impact-of-ai-on-fraud-and-scams.pdf

useful for catching new or evolving schemes[4]. While supervised ML is widely used, more advanced deep learning models and semi-supervised approaches are emerging as data availability grows, historically their adoption was limited due to complexity and data requirements.

8.2 *Behavioural Analytics and Biometrics*
Financial institutions increasingly leverage AI to analyse user behaviour and device data for subtle fraud indicators. Behavioural biometrics create a "digital fingerprint" of how a customer typically interacts, and then detect deviations that suggest fraud [5]. For example, AI systems monitor how a phone is held (orientation, movement), typing cadence and touchscreen pressure, typical login times, device ID, IP address, etc. Unusual patterns, such as a customer suddenly using a new device, typing with a different rhythm, or copying-and-pasting basic information, can raise real-time flags[6]. Such models continuously learn from every legitimate and fraudulent interaction, improving accuracy with each confirmed fraud incident. Major UK banks employ these techniques; in fact, 9 of the 10 largest UK banks utilise a leading AI-powered "digital identity" system (Threat Metrix) to profile user behaviour and spot anomalies[7].

8.3 *Natural Language Processing (NLP)*
AI text analysis is used in fraud and financial crime detection for tasks like scanning communications and documents. NLP models can screen vast unstructured data – emails, chat logs, insurance claims, news feeds, KYC documents – to identify risk-relevant keywords, sentiments or inconsistencies that might indicate fraud or illicit activity[8]. For example, banks use NLP to detect phishing patterns or social engineering content in written messages, and to monitor transaction descriptions or social media for scam indicators. In anti-money laundering (AML) compliance, NLP helps automate customer due diligence (e.g. adverse media screening) by sifting through news and legal texts for negative mentions of clients [9].

8.4 Network and Graph Analytics
Many fraud schemes involve networks of accounts or entities (e.g. money mule networks, coordinated insurance claims, shell companies for laundering). AI-driven network analytics map relationships among customers, accounts, transactions, and other data points to detect organised fraud rings that single-account analysis might miss. Graph algorithms and even graph neural networks (GNNs) can identify suspicious linkages – for instance, shared contact details, IP addresses, or transaction patterns linking seemingly unrelated accounts. In practice, this is used to find rings of fraudulent insurance claims or webs of transactions indicative of money laundering. The UK Insurance Fraud Bureau's new AI system IFB Exploration exemplifies this. It provides *"advanced network detection"* across insurers' combined data, flagging networks of linked claims and delivering more than 40 fraud network alerts weekly for investigation [10]. This shared AI platform, powered by graph analytics, enables insurers to uncover organised fraud faster and refer evidence to police.

---

[4] https://www.nature.com/articles/s41599-024-03606-
[5] https://www.information-age.com/artificial-intelligence-helps-slash-fraud-at-uk-banks-123510779
[6] See 5.
[7] See 5.
[8] https://ripjar.com/blog/regulatory-perspectives-on-ai-in-financial-crime/#
[9] See 8.
[10] https://www.insurancefraudbureau.org/media-centre/ifb-news/2023/new-ai-solution-ifb-exploration-drives-up-fraud-detection-for-insurers/#:~:text=IFB%20Exploration%20provides%20advanced%20network,contextual%20insights%20as%20they%20emerge

8.5 *Advanced Pattern Recognition (Voice, Vision, etc.)*
Cutting-edge AI tools are tackling novel fraud vectors. Voice analytics can now detect synthetic or suspicious voices – for example, identifying if a fraudster is using voice-cloning AI to impersonate a customer. Banks are beginning to use AI-driven voice biometrics to verify callers and spot signs of *"deepfake"* audio in scam calls[11]. Similarly, computer vision techniques help verify documents and images: AI can scrutinise customer-submitted ID photos or claim images for signs of manipulation (Photoshop or deepfake image artifacts)[12]. Such AI-based image forensics are increasingly important as criminals use AI to forge documents and deepfake videos. Across industry, organisations are exploring all these AI capabilities, voice, vision, text, and transaction data, to strengthen fraud detection from every angle.

8.6 Overall, AI's ability to analyse huge volumes of data and detect subtle anomalies far faster than humans makes it invaluable in combating fraud. AI systems, like *Cleafy* that take a cyber approach, using indicators from full-traffic analysis to pre-emptively stop fraud and scams[13], can monitor *every* login, payment, or message in real-time and cross-reference countless data points - a task impossible to do manually. Banks report that machine learning has reduced false positives (so legitimate customers aren't unnecessarily flagged) while catching more fraud; as one UK bank's Head of Fraud noted, *"machine learning techniques are generally already embedded in our fraud detection systems, reducing false positive rates and driving efficiency… while improving our ability to spot suspicious activity"*[14]. These technologies form the backbone of modern fraud prevention in financial services.

Industry Applications and Case Studies

9. Banks are using AI to monitor transactions and customer behaviour continuously, stopping fraud *before* losses occur. A consortium of nine UK banks (including major firms like Lloyds Bank, NatWest, Monzo, Halifax, Bank of Scotland, and TSB) recently partnered with Mastercard to deploy an AI-powered fraud risk system for real-time payments [15]. This system traces funds moving through networks of accounts (often mule accounts used by criminals) and analyses factors like account history, payment values, and account names to predict if a payment is likely fraudulent[16]. TSB, one of the early adopters, reported it "dramatically increased" fraud detection within the first four months of using this AI tool. Mastercard estimates that if all UK banks used the system with similar success, it could prevent nearly £100 million in scam payments annually across the UK[17].

10. Another example is a pilot by Pay.UK (the UK's payment authority) with Visa's AI fraud solution, which gave a multi-bank view of account-to-account payment risk. In tests, Visa's AI was able to intercept 54% of fraudulent transactions that had slipped through individual banks' defences, demonstrating the power of cross-institution data sharing[18]. Visa projected that scaling this solution could prevent up to £330 million in authorised push payment scam losses

[11] https://www.pwc.co.uk/forensic-services/assets/impact-of-ai-on-fraud-and-scams.pdf
[12] See 11.
[13] https://www.cleafy.com/proactive-banking-fraud-defence
[14] https://www.pwc.co.uk/forensic-services/assets/impact-of-ai-on-fraud-and-scams.pdf
[15] https://www.fintechfutures.com/2023/07/nine-uk-banks-tap-mastercard-ai-to-fight-payment-fraud/#
[16] See 15.
[17] See 15.
[18] https://corporate.visa.com/content/dam/VCOM/corporate/products/documents/visa-protect-for-a2a-payments-pay.uk-case-study.pdf#:~:text=Through%20the%20pilot%20with%20Pay,UK%20and%20industry

per year in the UK. These cases highlight how AI can correlate data across banks and in real-time *authorisation flows* to stop scams (like impersonation scams or invoice fraud) that are hard to detect with siloed, manual checks.

11. Digital banks and fintech platforms often lead in AI adoption, given their tech-first model. UK neobank Monzo has invested heavily in machine learning for fraud prevention. Monzo developed an AI-driven system that scores transactions in real time, enabling it to detect and block suspicious payments within seconds[19]. By training models on historic transaction data, Monzo's system learned to differentiate genuine customer behaviour from fraud patterns. The results have been striking. Monzo reportedly achieved an 80% reduction in fraud losses after implementation, while detecting 95% of fraudulent transactions almost immediately as they occur[20]. The bank also managed to cut false positives (legitimate transactions incorrectly flagged) by about 50%, thus improving customer experience. These improvements not only save money but also boost customer trust and convenience.

12. In an effort to combat the rising threat of scams, international money transfer app, Wise, launched a new initiative called the 'Scam Safe Space.' This platform aims to help people share their experiences of scams without fear of judgment, raising awareness and educating others on how to avoid being targeted. Wise, reports that its investment in cutting-edge detection technology, including AI detection technologies, has reduced fraud volumes by approximately 70% over the past year[21]. But Aaron Wilson, head of fraud prevention at Wise, explained that prevention necessitates more than just technology, *"While technology can help prevent scams it also requires effective education and talking about your scam experience with family and friends is a great form of education,"* he said[22]. Financial institutions such as Wise, recognise that AI is a tool that needs to be utilised within a holistic approach to fraud prevention and detection.

13. The insurance industry is tapping AI to spot fraudulent claims and underwriting fraud. Insurers in the UK collaborate through the Insurance Fraud Bureau (IFB), which launched an AI-powered platform called *IFB Exploration* in 2022. This system, built with Shift Technology, serves as a shared industry solution using AI and network analytics to uncover fraud rings across motor, property, and liability insurance lines[23]. Over the past year, IFB Exploration led to a six-fold increase in fraud searches by insurers (now 3,500+ searches per month) as companies mine combined data for connections (. It generates around 40 alerts of suspected fraud networks each week, yielding new intelligence that is passed to law enforcement. For example, the AI might find that multiple seemingly unrelated claims (perhaps across different insurers) actually link to the same organised group or pattern – a level of insight that individual insurers wouldn't have on their own. By sharing this AI tool, insurers have *"seen a big rise in collaboration and dissemination of vital insights across the counter-fraud community"*,

[19] https://headofai.ai/monzo-ai-driven-fraud-detection-in-digital-banking/#:~:text=Monzo%2C%20a%20digital%20banking%20platform,detecting%20fraudulent%20activities%20within%20seconds

[20] https://headofai.ai/monzo-ai-driven-fraud-detection-in-digital-banking/#:~:text=

[21] https://www.express.co.uk/finance/personalfinance/2039523/scam-fraud-victims-silence

[22] See 22.

[23] https://www.insurancefraudbureau.org/media-centre/ifb-news/2023/new-ai-solution-ifb-exploration-drives-up-fraud-detection-for-insurers/#:~:text=Utilised%20exclusively%20by%20IFB%20members%2C,and%20adapt%20to%20evolving%20threats

according to the IFB's director [24]. The result is faster investigations and more fraudsters being caught, helping protect honest policyholders.

14. Combating money laundering is a major aspect of financial crime prevention. Banks have traditionally relied on rule-based transaction monitoring systems, which often generate large volumes of false-positive alerts that human analysts must review. AI is now being applied to make AML monitoring smarter and more risk-based. Several large banks have reported success using machine learning to prioritise alerts and reduce false positives by analysing patterns in historical Suspicious Activity Reports (SARs). For instance, HSBC has publicly discussed using AI to sift through transactions and identify truly suspicious anomalies, thereby cutting the number of irrelevant alerts and focusing investigators on the most probable cases (though exact figures are often confidential). In one case study, a global retail bank used an AI solution that reduced AML alert false positives by 20–30%, freeing compliance teams to concentrate on genuine threats [25].

15. A growing threat in the UK is APP fraud, where customers are tricked into sending money to fraudsters (e.g. through impersonation scams). Because the customer initiates the payment, traditional security (like 2FA) might not flag it. AI has become a crucial defence here. The earlier-mentioned Mastercard and Visa solutions are directly aimed at APP fraud: by analysing the payment metadata and history in real time, they can flag a payment as likely scam (for example, if the payee has characteristics matching known mule accounts, or if the customer's behaviour deviates from normal). UK banks are also building their own models; for instance, some banks use recipient account risk scoring (aggregating data on accounts known for fraud) and combine it with sender behaviour analysis. The results of these initiatives are promising – UK Finance reported a slight dip in fraud losses in 2023, attributing it partly to enhanced scam detection outpacing the thieves[26].

16. Looking ahead, the Financial Services and Markets Act 2023 will require banks to reimburse APP fraud victims, which further incentivises banks to invest in AI to stop these payments before they go through. The industry's use of AI in this area not only prevents losses but also protects customers from the trauma of being scammed, reinforcing trust in digital banking.

17. These examples illustrate that AI is making a tangible impact: detecting fraud faster and more accurately, reducing manual workloads, and adapting to new fraud tactics. From large incumbent banks to fintech startups and insurers, the consensus in the industry is that AI-based fraud prevention is not just an add-on but a necessity in an era of increasingly digital and sophisticated financial crime.

The Perspective of Leaders in Financial Services.

18. This research into the future of fraud and Artificial Intelligence includes in-depth, anonymous, interviews with Heads of Fraud from three UK Financial institutions and two

[24] See 23.

[25] https://www.niceactimize.com/Lists/CustomerSuccesses/Attachments/53/aml_case_study_bank_reduces_false_positives_33_percent.pdf#:~:text=33,the%20significant%20backlog%20which

[26] https://www.information-age.com/artificial-intelligence-helps-slash-fraud-at-uk-banks-123510779/#:~:text=accounts%2C%20login%2C%20make%20payments%2C%20and,detection%20methods%20outpaced%20the%20thieves

Subject Matter Experts from AI Technology providers. This next section details their perspectives on AI in financial services for fraud prevention and detection.

19. AI is increasingly being adopted across financial institutions for the purposes of fraud detection and prevention, and has been used in conjunction with traditional rules-based systems for decades. Early applications were particularly focused on payment fraud, where AI supported decision-making within rigid rule engines. These systems laid the foundation for today's more dynamic approaches but were limited by their dependence on structured data and predefined thresholds. One organisation has implemented AI-enhanced transaction monitoring and risk scoring engines, capable of scanning billions of transactions to identify suspicious patterns. A senior fraud professional noted that their AI-supported fraud policy engines had evolved significantly in recent years, stating, "*We've matured our fraud policy engines to do transaction screening and monitoring… using scoring techniques to scan billions of events on a daily, weekly, monthly basis."* This capability is central to their five-pillar fraud management framework: prediction, prevention, detection, response, and recovery.

20. A fundamental principle has remained unchanged: AI is only as effective as the data it ingests. "*Without good data sources, technology can't do what it's meant to do,"* noted one specialist. Poor data integration and departmental silos continue to limit the potential of AI in many institutions. However, AI's evolution, particularly through machine learning and real-time analytics, has transformed its utility. It now offers real-time fraud detection capabilities that adapt to evolving criminal behaviours.

21. Today, AI systems can process and analyse data with a speed and scale far beyond human capabilities. As one specialist described, "*It's like cracking the Enigma code - once the machine can identify certain patterns, it can make faster, more accurate decisions."* This shift enables AI to detect subtle anomalies and behavioural patterns that might otherwise go unnoticed.

22. Yet, significant challenges remain. AI's power to automate and detect is hindered by fragmented organisational structures and legacy infrastructure.

23. AI's effectiveness is also jeopardised by rising threats such as AI-generated synthetic identities and deepfake fraud, which require equally sophisticated countermeasures. "*It's an arms race,"* another contributor observed, as both sides (the defenders and the fraudsters) employ increasingly complex technologies.

24. A promising opportunity lies in borrowing strategies from other industries. For example, the oil sector has used AI for years to optimise pricing using fuzzy logic and real-time data analysis. Similarly, AI in finance must evolve to consider context-rich, multi-source data inputs.

25. One expert warned that financial institutions must break down internal silos and foster cross-departmental integration. "*Fraudsters exploit gaps between departments,"* they noted, underscoring the importance of holistic AI implementation.

26. AI's future, according to several contributors, is about partnership. The most effective approach is not AI replacing humans, but AI augmenting human decision-making. Routine, repetitive tasks should be delegated to AI, allowing human analysts to focus on strategic decisions and complex casework. *"AI will help reduce repetitive decision-making, allowing humans to use their creativity and critical thinking to develop new ways of winning the battle against fraudsters."*

27. This approach was echoed by another industry leader, who noted that the greatest potential of AI lies in its ability to enhance, not replace, human oversight. *"People are afraid that jobs will be replaced,"* they remarked, *"but technology should be viewed as a tool to enhance human capabilities."*

28. AI should empower analysts to spend less time on mundane decisions and more time on problem-solving and consumer protection. Organisations are developing multi-stream research projects, including those focused on scams, culture, and neurodivergence, to better understand how AI can support targeted and inclusive fraud prevention strategies.

29. Importantly, the sector should actively encourage innovations that originate from people-first approaches and are grounded in ethical AI use. For example, platforms like *Ask Silver* [27]demonstrate how AI can support those at risk of scams by guiding individuals through reporting and recovery in accessible, human-centred ways. Similarly, technology from organisations like *Lynx Tech*[28], which emerged from public-private partnerships between universities and financial services, offers evidence-based, research-informed tools for real-time fraud detection. These examples show that effective innovation in this space often stems from close collaboration between researchers, practitioners, and those with lived experience, ensuring that AI systems are responsive to real-world needs and grounded in trust.

AI and Business Culture in the Financial Services Sector

30. This research into the future of fraud and Artificial Intelligence includes analysis of a survey completed by 150 financial services staff, including 20% identifying as senior leadership (Head of Fraud, Money Laundering Regulatory Officer (MLRO) or similar), and 25% as fraud intelligence analysts/ investigators. The remaining 55% represented all other areas of financial services, with between 3-15years plus experience working in the sector.

31. Despite the growing presence of AI, understanding and confidence in its use remain limited among many professionals. Survey data reveals that only 18% of respondents felt confident using AI tools in fraud detection, while 15% indicated they did not understand these tools at all.

32. 81% of respondents believed that additional training on AI-driven fraud detection tools would enhance their effectiveness, particularly in handling complex or sensitive cases. One analyst summarised this by saying, *"We're using tools we don't fully understand—there's a need for structured upskilling if we're going to get ahead of fraud."*

33. When asked about the integration of AI into their workflows, fraud professionals highlighted both the benefits and the risks. One interviewee remarked that "*fraudsters are adapting very quickly using AI themselves, we're seeing much more sophisticated falsified documentation, potentially AI-generated, and it's becoming increasingly difficult to differentiate."*

34. Another interviewee observed the emergence of *"cat-and-mouse dynamics,"* where fraudsters iteratively modify their tactics in response to changes in fraud controls. One institution documented hundreds of variations in fraudulent applications - indicating fraudsters' use of A/B testing to explore vulnerabilities in automated defences.

[27] https://www.ask-silver.com/
[28] https://lynxtech.com/

35. Additional survey comments noted concerns about false positives. One respondent stated, "*AI helps flag more, but not always accurately, it's creating workload without always reducing risk.*" Another added, "*There are days when we feel we're firefighting our own systems more than we're fighting the fraudsters.*"

36. In terms of consumer impact, especially concerning vulnerable customers, AI has the potential to offer tailored protections by identifying high-risk behaviours and patterns of exploitation. However, without robust human oversight, AI also risks amplifying bias or misclassifying legitimate behaviours. One senior respondent noted that distinguishing between deliberate fraud and financial distress is often complex: *"The line between a fraudster and a customer who just doesn't repay is thin. You need AI to help, but you also need a human to contextualise the intent."*

37. Another expert reinforced this, pointing to the growing importance of understanding *"hidden vulnerabilities,"* such as neurodivergence, which can impact how individuals are targeted or misjudged by AI systems. They argue for adaptive fraud systems informed by interdisciplinary research, and a need for AI tools that reflect the diversity of the user base they serve. One participant commented, "*We need AI to understand not just fraud patterns, but also consumer behaviour that's unusual but not malicious*."

38. Cultural shifts within organisations appear to play a vital role in improving fraud detection and prevention. A senior fraud leader stated, "*Our management didn't always listen to fraud warnings, but after a few reputational hits and financial losses, they began to factor fraud into product decisions from the start."* Similarly, increased fraud awareness, both internally and among consumers, has helped organisations adapt more quickly to emerging threats.

39. Despite technological advancements, key adoption barriers persist. Many institutions struggle with integrating AI tools into legacy systems or justifying the investment in the absence of immediately measurable returns. In addition, regulatory ambiguity continues to hinder confidence. "*We often face pushback from the business unless there's a significant fraud loss,"* one practitioner explained. This highlights the need for regulatory clarity that supports innovation while enforcing strong governance.

40. Criminal innovation is also accelerating. All interviewees recounted instances where fraudsters rapidly adapted to defensive measures, such as changing browser types, altering visual patterns in photos, and manipulating metadata to bypass AI checks. *"We block one tactic, and within days, they reconfigure the attack,"* one expert shared. This dynamic underscores the need for agile, data-driven, and collaborative approaches to AI in fraud management.

Recommendations

41. Given these findings, it is vital to recognise the vital role that highly skilled professionals play in the future of AI in financial services. However, professionals tasked with preventing and detecting financial crime in our financial service institutions don't feel adequately supported or skilled enough to utilise AI effectively. As such, we recommend sector-wide training programmes to build AI literacy among fraud professionals. This should be paired with new certification standards that reinforce minimum capabilities for working with AI systems.

42. Cross-sector data sharing must also be enhanced. Secure, anonymised consortiums would allow institutions to pool insights, identify trends earlier, and adjust models more effectively.

Several practitioners emphasised the importance of industry collaboration, echoing that "*fraudsters share information across borders - we need to match that level of cooperation*."

43. Regulatory guidance should be created and regulary updated to promote explainability and transparency in high-risk AI applications. Existing financial crime frameworks should be expanded to include AI-specific indicators. At the same time, AI systems must be designed to protect vulnerable consumers, with human review mandated for flagged transactions involving those at heightened risk.

44. The government should consider incentivising innovations that take a people-first approach while leveraging AI as an efficient backend tool. Solutions such as *Ask Silver*, *Cleafy,* and *Lynx Tech,* and the practical implementation of AI by financial institutions such as *Monzo* and *Wise* illustrate the kind of practical, ethical, and research-informed development that can improve outcomes for both financial institutions and consumers.

45. Lastly, public education is vital. Consumer awareness of how AI protects them, and how criminals may exploit new technologies, can strengthen resilience. Financial institutions and regulators should support ongoing campaigns that educate the public on fraud risks and digital safety.

46. The responsible adoption of AI in fraud prevention holds tremendous promise for protecting consumers and reducing crime. Yet, the technology must be paired with education, oversight, and cross-sector cooperation to ensure it does not inadvertently harm those it seeks to protect. With thoughtful regulation and investment in skills, the UK financial services sector can lead globally in the ethical deployment of AI for fraud prevention. As demonstrated by research, expert insights, and practical examples, a true partnership between humans and AI, where one enhances the effectiveness of the other, offers the most resilient defence against evolving fraud threats.

April 2025