# Experts warn 2025 is pivotal year for adaptive fraud prevention as remote purchase scams surge



In a climate marked by rapid technological advancement, experts assert that 2025 will be pivotal for adaptive fraud prevention methods. As fraud evolves, propelled largely by generative AI, traditional static prevention techniques are becoming increasingly inadequate. The crux of the issue, according to UK Finance’s latest annual fraud report, is that fraud is now the most prevalent crime in the UK, resulting in losses exceeding £1.1 billion in 2024. While the report indicated a slight decline in authorized push payment (APP) fraud, remote purchase fraud surged, filling the gap left by such decreases.

The need for a dynamic approach to fraud prevention has never been more pressing. Ben Donaldson, managing director of economic crime for UK Finance, emphasised in the report that addressing fraud should be viewed as a continual process. "Rather than trying to ‘solve’ fraud, our objective should be to protect as many people as possible by reducing and managing the evolving threat," he stated. This perspective highlights the necessity for a collaborative and strategic response that encompasses technology, telecommunications, and public sectors as a means of fortifying the UK's defenses against fraud.

In parallel with industry concerns, Jonathan Frost, Director of Global Advisory for EMEA at BioCatch, remarked on the resilience of fraudsters. He noted that the persistent nature of these criminal activities necessitates collective innovation and adaptive strategies. "While industry is holding its own against the rising tide of fraud, the gains made by fraudsters demonstrate that the fraud threat is persistent," Frost said. He underscored the need for a comprehensive national fraud strategy that prioritises prevention and accountability across sectors.

The latest insights from the financial sector reveal that while APP fraud—where victims are tricked into making payments—dropped to £450 million, unauthorized fraud escalated dramatically. In fact, losses from unauthorized fraud reached £722 million and incidents rose by 14%, reaching over 3.13 million cases, largely thanks to the proliferation of remote purchase scams exploiting stolen card information. Experts are now advocating for systemic reforms that include heightened involvement from tech and telecom sectors to address these evolving threats.

Moreover, the conversation around technology’s role in thwarting fraud is gaining momentum. Trends highlighted at the recent Fraud Prevention Summit underscored the implementation of AI-driven fraud detection systems and behavioural analytics to monitor transactions in real time. Biometric authentication and multi-factor authentication are now standard tools employed by financial institutions to protect customer accounts, effectively ensuring that only legitimate users access sensitive financial data.

Other players in the technology space are also making strides in fraud prevention. Feedzai recently announced the launch of Feedzai IQ, which employs artificial intelligence while prioritising customer privacy. The product aims to harness extensive network insights to bolster detection accuracy, addressing the urgent need for enhanced fraud prevention measures. As Pedro Barata, chief product officer at Feedzai, stated, "The true power of AI is only unlocked through access to meaningful, high-quality data."

In a similar vein, Spain's Facephi has introduced a real-time fraud prevention solution that utilises behavioural biometrics to create unique user profiles based on digital interactions. General Manager Jorge Sanz described the aim to develop a "cyber-DNA" that differentiates legitimate users from potential fraudsters based on various contextual signals.

Amid these innovations, there are also calls for financial institutions to adopt federated learning in their fraud detection systems. This collaborative approach allows the sharing of valuable insights without compromising customer data, further strengthening defences against sophisticated fraud techniques.

As the landscape shifts, industry leaders are advocating for a transition from static to adaptive fraud prevention models that utilise comprehensive data analytics and real-time monitoring capabilities. SEON’s recent findings highlight that two-thirds of organisations are prioritising real-time transaction monitoring to keep pace with evolving risks.

The stakes are high, and as new fraud strategies emerge, the focus remains on creating a robust system that adapts to threats in real time. With collaboration between various sectors viewed as pivotal, the commitment to refining fraud prevention strategies is crucial for safeguarding consumers against the relentless rise of fraud in an increasingly digital world.

### 📌 Reference Map:

* Paragraph 1 – [[1]](https://www.biometricupdate.com/202506/2025-is-the-year-of-adaptive-fraud-prevention-say-experts), [[2]](https://www.ft.com/content/c877784c-f416-4c7b-943b-dfb35a01233c)
* Paragraph 2 – [[1]](https://www.biometricupdate.com/202506/2025-is-the-year-of-adaptive-fraud-prevention-say-experts), [[6]](https://thepaymentsassociation.org/article/tackling-fraud-in-2025-fighting-ai-fraud-with-new-ai-models/)
* Paragraph 3 – [[2]](https://www.ft.com/content/c877784c-f416-4c7b-943b-dfb35a01233c), [[4]](https://fpsummit.co.uk/briefing/fraud-prevention-what-did-2024-deliver-and-where-are-we-going-next/)
* Paragraph 4 – [[5]](https://www.ukfinance.org.uk/news-and-insight/blog/how-federated-learning-strengthens-fraud-detection-in-2025), [[3]](https://www.sas.com/en_gb/news/press-releases/2024/february/study-8-in-10-fraud-fighters-expect-to-deploy-generative-ai-by-2025.html)
* Paragraph 5 – [[1]](https://www.biometricupdate.com/202506/2025-is-the-year-of-adaptive-fraud-prevention-say-experts), [[5]](https://www.ukfinance.org.uk/news-and-insight/blog/how-federated-learning-strengthens-fraud-detection-in-2025)
* Paragraph 6 – [[5]](https://www.ukfinance.org.uk/news-and-insight/blog/how-federated-learning-strengthens-fraud-detection-in-2025), [[3]](https://www.sas.com/en_gb/news/press-releases/2024/february/study-8-in-10-fraud-fighters-expect-to-deploy-generative-ai-by-2025.html)
* Paragraph 7 – [[4]](https://fpsummit.co.uk/briefing/fraud-prevention-what-did-2024-deliver-and-where-are-we-going-next/), [[6]](https://thepaymentsassociation.org/article/tackling-fraud-in-2025-fighting-ai-fraud-with-new-ai-models/)
* Paragraph 8 – [[6]](https://thepaymentsassociation.org/article/tackling-fraud-in-2025-fighting-ai-fraud-with-new-ai-models/), [[7]](https://www.finextra.com/blogposting/27344/fraud-in-2025-five-trends-that-are-on-the-rise)

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

## Bibliography

1. <https://www.biometricupdate.com/202506/2025-is-the-year-of-adaptive-fraud-prevention-say-experts> - Please view link - unable to able to access data
2. <https://www.ft.com/content/c877784c-f416-4c7b-943b-dfb35a01233c> - In 2024, fraudsters stole £1.17 billion from UK consumers, reflecting persistent criminal activity despite increasing preventative efforts, according to UK Finance's annual report. While authorised push payment (APP) fraud losses dropped slightly to £450 million due to heightened consumer awareness and tech investments, unauthorised fraud rose to £722 million, driven by new scams. APP fraud involves tricking victims into transferring money into fake accounts, whereas unauthorised fraud includes illicit use of bank and card details. Investment fraud was the most common APP scam, with total losses increasing despite fewer cases. Unauthorised fraud rose 14% to 3.13 million incidents, mainly from remote purchase fraud using stolen card data. The Payment Systems Regulator's October mandate for mandatory reimbursement of APP fraud victims led to an 86% return rate within three months. More than 98% of unauthorised fraud victims were fully refunded. Experts like BioCatch's Gadi Mazor and UK Finance’s Ben Donaldson called for a systemic approach, pushing for greater involvement from the technology and telecom sectors and enhanced collaboration between public and private stakeholders to combat fraud effectively. Fraud remains a significant threat that funds serious criminal activity both domestically and internationally.
3. <https://www.sas.com/en_gb/news/press-releases/2024/february/study-8-in-10-fraud-fighters-expect-to-deploy-generative-ai-by-2025.html> - A global survey by the Association of Certified Fraud Examiners (ACFE) and SAS reveals that 83% of anti-fraud professionals anticipate incorporating generative AI into their fraud prevention strategies within the next two years. This finding underscores the growing enthusiasm for AI technologies in combating fraud. The 2024 Anti-Fraud Technology Benchmarking Report, based on insights from nearly 1,200 ACFE members surveyed in late 2023, highlights a significant increase in interest towards artificial intelligence and machine learning technologies. The report indicates that fraud fighters are increasingly recognising the potential of AI to enhance fraud detection and prevention efforts, reflecting a broader trend towards adopting advanced technologies in the fight against financial crimes.
4. <https://fpsummit.co.uk/briefing/fraud-prevention-what-did-2024-deliver-and-where-are-we-going-next/> - The 2024 Fraud Prevention Summit highlighted several key trends in the UK's retail and banking sectors. AI-driven fraud detection and behavioural analytics are being leveraged to monitor customer habits and flag suspicious activities in real time. Biometric authentication and Multi-Factor Authentication (MFA) have become standard to secure logins and transactions, ensuring only legitimate users access sensitive financial information. Blockchain technology is emerging as a tool for fraud prevention by decentralising transaction data and creating transparent, immutable ledgers, making it nearly impossible for fraudsters to manipulate records. Real-time transaction monitoring, coupled with adaptive risk scoring, is increasingly used to assess the risk of each transaction based on contextual factors, reducing fraud attempts while maintaining a smooth experience for low-risk customers. The outlook for 2025 anticipates increased reliance on AI-driven analytics, blockchain expansion, and a focus on data-sharing collaborations between institutions to strengthen defences against fraud.
5. <https://www.ukfinance.org.uk/news-and-insight/blog/how-federated-learning-strengthens-fraud-detection-in-2025> - UK Finance discusses the role of federated learning in enhancing fraud detection. Federated learning enables financial institutions to collaborate on fraud prevention while protecting sensitive customer data. This approach allows institutions to share insights and improve fraud detection models without exposing individual datasets, thereby strengthening collective defences against fraud. The blog emphasises the importance of adopting innovative technologies like federated learning to stay ahead of increasingly sophisticated fraudsters in 2025.
6. <https://thepaymentsassociation.org/article/tackling-fraud-in-2025-fighting-ai-fraud-with-new-ai-models/> - The Payments Association explores the evolving landscape of AI-driven fraud in 2025. With fraudsters increasingly adopting AI tools, banks are urged to implement adaptive AI models to detect and prevent scams in real time. The article highlights the challenges posed by sophisticated AI-enabled fraud tactics and the necessity for financial institutions to enhance their fraud detection capabilities to keep pace with these evolving threats.
7. <https://www.finextra.com/blogposting/27344/fraud-in-2025-five-trends-that-are-on-the-rise> - Finextra outlines five emerging fraud trends anticipated in 2025. These include the rise of AI-driven fraud, increased cross-border fraud, and the need for businesses to respond quickly and effectively to these threats. The article emphasises the importance of leveraging advanced technologies and real-time data analytics to detect and mitigate fraud as it happens, highlighting the global nature of digital transactions and the ease with which fraudsters can exploit vulnerabilities across different jurisdictions.