# AI drives a new arms race in fraud detection and tactics



In a landscape increasingly shaped by advances in technology, artificial intelligence (AI) is proving to be a pivotal force in fraud detection. As businesses welcome AI's capabilities to identify fraudulent activity swiftly and precisely, they simultaneously face an escalating challenge: fraudsters are employing the same technologies to enhance their scams, which complicates traditional detection efforts.

The publication Biometric Update reports on an upcoming panel discussion that aims to delve into this complex dynamic. Scheduled to feature several experts in the field, the webinar will explore how AI is being utilised on both sides of the fraud spectrum—by those aiming to prevent fraud and those seeking to perpetrate it.

Among the key figures participating in the discussion is Stephen Thwaits, Senior Vice President of Decision Innovation at AuthenticID, and Ben Davey, Co-founder and Vice President of Product at Darwinium. Chris Burt, Managing Editor at Biometric Update, will serve as the moderator for the event.

The panel is anticipated to provide insights into several crucial areas. Participants will learn about the real-time applications of AI in enhancing security measures and identifying fraud. There will also be a focus on the innovative tactics employed by fraudsters that leverage AI, creating an intricate ongoing battle between fraud prevention methods and the increasingly sophisticated techniques used by fraudsters.

Additionally, the session will highlight the challenges that businesses and individuals face in detecting AI-driven fraud, signalling a need for continual adaptation in detection strategies. The discussion will culminate in consideration of what the future may hold for fraud detection, particularly in the context of the growing sophistication of both AI tools and fraudulent activities.

The insights gained from this panel are expected to shed light on the evolving interplay between technology and fraud, equipping participants with knowledge that may aid in the arms race against fraudulent practices in a rapidly digitising world.

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

## Bibliography

1. <https://www.axios.com/2025/03/11/visa-scam-disruption-practice-fraud> - Visa has established a new initiative aimed at detecting and dismantling online scammers to protect customers, addressing the growing scam ecosystem. This effort arises as consumers lost over $1 trillion to scams globally last year, and law enforcement struggles to manage the sheer volume of online scams. Modeled after threat intelligence units in cybersecurity, Visa's team proactively studies and disrupts scam operations, having already thwarted over $350 million in attempted fraud in 2024. The team focuses on expanding intelligence-gathering, accelerating scam takedowns, and investing in AI and automation to enhance detection capabilities. This initiative underscores Visa's commitment to safeguarding its customers and platforms against fraud.
2. <https://www.ft.com/content/b7674c60-8234-432a-b70b-b5b48a98cf32> - In the rapidly changing IT industry, despite some technologies like blockchain and the metaverse struggling, others such as artificial intelligence, cloud computing, and workflow automation have gained mainstream traction. These three technologies are prominent among fast-growing European businesses. For example, Paris-based start-up Veesion uses AI-powered surveillance to reduce shoplifting significantly, helping over 4,000 stores across 25 countries. Meanwhile, SourceWhale uses AI to enhance workflow automation for recruitment agencies, reducing administrative burdens and improving efficiencies. Its software is now widely used in the recruitment industry, contributing to rapid revenue growth. Additionally, Polish company Solidstudio is developing AI technology to prevent fraud in the electric vehicle sector. This technology-centric evolution highlights the versatility and transformative impact of AI, cloud computing, and automation in modern business operations.
3. <https://www.ft.com/content/577dff0d-b7a0-4bc3-a1b1-3ca828e5ba18> - The issue of who should bear financial responsibility for cyber scams, especially in the face of advancing AI and quick payment networks, is unraveling across various sectors. California lawyer Christopher Pitet’s recent loss of $59,517.50 to a hacker highlights the complexity of cyber scams where banks, governments, and technology companies all play roles. Pitet's lawsuit against Citibank, which refused to refund the fraudulent payment, exemplifies the ongoing debates and legal battles. Fraud loss in the US reached $158bn in 2023 due to AI-driven scams such as deepfakes and authorized push payment fraud. UK regulations cap bank liability for such frauds at £85,000, while Australia's government considers holding tech companies accountable. In the US, proposals for similar regulations face political contention, with banks arguing against bearing full liability, citing potential cost impacts on services. The growing sophistication of fraud techniques suggests a need for collaborative measures among banks, tech firms, and other stakeholders to protect consumers and mitigate losses.
4. <https://newsroom.mastercard.com/news/press/2024/may/mastercard-accelerates-card-fraud-detection-with-generative-ai-technology/> - Mastercard is using generative AI to double the speed at which it can detect potentially compromised cards, further protecting cardholders and securing the ecosystem. Fraudsters steal millions of payment card numbers through spyware, malware, and other clandestine practices such as card skimming. In a bid to sell this data to other criminals, they place part of the 16-digit numbers on illegal websites. Mastercard, a world leader in cyber security, is now better able to predict the full card detail of these compromised cards on its network, enabling banks to block them far faster than previously.
5. <https://www.reuters.com/world/us/bankman-fried-lieutenant-builds-fraud-detection-tool-prosecutors-2024-11-13/> - Gary Wang, a former executive at FTX who once helped Sam Bankman-Fried steal billions from cryptocurrency customers through manipulated computer code, is now creating fraud detection software for the U.S. government. This initiative aims to assist prosecutors in detecting fraud in the stock market and cryptocurrency exchanges. Federal prosecutors highlighted Wang's cooperation and his proactive use of skills in a recent court filing, as they urge for leniency in his sentencing, scheduled for November 20. Wang's efforts come as part of his collaboration with authorities following FTX's collapse in November 2022. Bankman-Fried is currently serving a 25-year prison sentence, convicted of stealing $8 billion to support his hedge fund, Alameda Research. Other key figures involved, including Caroline Ellison and Nishad Singh, have already faced their penalties, with Wang being the last to be sentenced.
6. <https://www.theglobaltreasurer.com/2025/03/21/how-ai-is-reshaping-fraud-detection-in-payments/> - Leading payment processors are embedding AI deeper into their fraud detection frameworks. Visa has deployed over 500 AI applications to enhance fraud detection and productivity. Over the past decade, the company has invested $3.3 billion in AI and data infrastructure, underscoring its commitment to combating financial crime. Visa’s AI models process over 500 million transactions daily, using machine learning to detect suspicious activity in real time. This level of automation allows Visa to prevent fraud before it impacts businesses and consumers. Mastercard is making similar strides. Its $2.65 billion acquisition of Recorded Future, a cybersecurity firm specializing in AI-driven threat intelligence, bolsters its ability to identify and mitigate cyber threats across its payment network. Mastercard’s AI tools analyze vast amounts of transactional data to spot anomalies, reducing the risk of account takeovers and synthetic identity fraud, where fraudsters create fake identities using real personal data.
7. <https://news.google.com/rss/articles/CBMiowFBVV95cUxONDM4aGpCYkpCSElRemF3NUdERkc2SjJZT3VUR2VwNUItTko0LXA1WlowUlJZSTJaYjY0NzB3MFZVdlhDRHNPdXJMc2swa0RoYUR5R1lDaEdtZmx6Z3hwX3NZU1BiMnlYRDBsTkUxbEl6YU51NGduTU5lalNGa0pNbWplMUUtZUhmTF91VUVZTXRTd2R2T1VtcWw3V3VlSmNkelA0?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data