# Financial institutions must innovate to combat AI-driven fraud effectively



Financial institutions (FIs) are confronting a rapidly evolving and increasingly complex fraud landscape, where the use of advanced technologies such as artificial intelligence (AI) is enabling criminals to circumvent traditional security measures. This scenario demands that FIs enhance their fraud protection capabilities while still providing a smooth and seamless experience for their customers.

The escalating threat linked to AI-driven fraud has been detailed by Jason Abbott, Director of Fraud Solutions at Provenir, who highlights how modern fraudsters combine sophisticated AI with social engineering to outsmart conventional fraud detection systems. Criminals acquire stolen credentials through online marketplaces and deploy readily accessible AI tools to target digital customer journeys more effectively. These AI applications can generate ultra-realistic digital identity documents for both synthetic and stolen identities, potentially bypassing existing digital identity verification methods.

Abbott explains that these AI tools employ authentic-looking templates that allow fraudsters to insert any credentials and photographs they choose. The outcome is a high-resolution image replicating genuine document security features and overlays. Moreover, such tools can simulate the process of these fraudulent documents being photographed by a mobile device, further complicating detection efforts by fraud teams.

Alongside technological advances in fraud tactics, consumer expectations for financial services have undergone a substantial transformation in the last decade. Processes that historically involved physical documentation and manual verification are now expected to be completed in real time. Today’s consumers anticipate instant account opening, identity verification, approval, and card activation via just a few taps on their smartphones. Immediate access to card transactions and digital payment services post-account creation is the new standard.

This acceleration has consequently squeezed the timeframe available for fraud teams to conduct thorough manual checks before accounts become vulnerable to exploitation. In response, fraud teams increasingly leverage sophisticated detection tools — like those used in payment channels — to identify anomalous behaviour by analysing multiple data points, including device information, behavioural biometrics, electronic identification and verification, and email and mobile intelligence. Aligning these data sources across different fraud channels enables more informed decisions at the application stage and continued monitoring during the high-risk initial months after account opening.

Abbott underscores the importance of real-time decisioning in preventing fraud affordably and effectively. He likens this process to assembling a jigsaw puzzle, stating: “With limited pieces, it’s challenging to perceive the complete picture. However, as more pieces are added, the clearer the overall image becomes.” A flexible decisioning platform that orchestrates internal and external data points enables financial institutions to make well-informed decisions quickly, thereby enhancing fraud prevention while reducing the need for manual interventions.

Artificial intelligence also plays a key role in automating labour-intensive tasks that typically strain fraud teams’ resources. AI’s capacity to learn from each processed event means that fraud detection systems can evolve alongside fraudsters’ changing tactics. Real-time data allows these AI models to continually refine their decisioning processes to optimise fraud alerts and reduce false positives. However, Abbott stresses the importance of aligning AI deployment with internal governance requirements, ensuring AI outputs are interpretable by humans and that useful data is not disregarded when manual decisions require further input.

Adopting a customer-centric approach to risk decisioning is crucial in today’s fight against fraud. Abbott emphasises that fraud mitigation must move beyond reactive measures to proactive, technology-driven strategies that continuously monitor customer behaviour throughout the entire lifecycle—from application through to ongoing high-risk event assessments. Newly opened accounts are especially susceptible to fraud, making the re-use of application data or rescreening of suspicious activity vital to identifying unusual behaviours, such as frequent changes to personal contact details or device use soon after account creation.

Through the integration of advanced technology, AI, and data analytics, financial institutions can maintain more effective fraud prevention strategies that reduce harm to legitimate customers while enhancing operational efficiency. Jason Abbott’s insights provide a detailed breakdown of how the evolving fraud landscape demands innovation, agility, and a comprehensive understanding of emerging threats for financial services to remain resilient.

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

## Bibliography

1. <https://www.pymnts.com/fraud-prevention/2024/71-percent-of-financial-institutions-turn-to-ai-to-fight-faster-payments-fraud/> - Supports the claim that financial institutions are increasingly adopting AI for fraud detection, with 71% of FIs now using AI/ML technologies to identify anomalies and patterns.
2. <https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2024/deepfake-banking-fraud-risk-on-the-rise.html> - Corroborates the escalation of AI-driven fraud threats, specifically mentioning the 700% increase in deepfake incidents in fintech during 2023.
3. <https://cybermagazine.com/cyber-security/authenticid-report-shows-deepening-financial-sector-threat> - Confirms the rise in deepfake-related fraud, noting that 46% of financial institutions experienced such incidents in the past year.
4. <https://www.biocatch.com/ai-fraud-financial-crime-survey> - Validates the prevalence of synthetic identity fraud and highlights that 48% of organizations use AI to detect these identities, aligning with the article's discussion of AI-generated fraudulent documents.
5. <https://www.rehmann.com/resource/ai-driven-financial-crimes-continue-to-raise-red-flags/> - Substantiates the financial impact of AI fraud losses ($12.3 billion in 2023) and discusses how generative AI and deepfakes enable increasingly adaptive financial crimes.
6. <https://www.pymnts.com/fraud-prevention/2024/71-percent-of-financial-institutions-turn-to-ai-to-fight-faster-payments-fraud/> - Reinforces the necessity of automated fraud detection systems mentioned in the article, emphasizing AI's role in real-time anomaly detection and pattern recognition.
7. <https://news.google.com/rss/articles/CBMirgFBVV95cUxOaDUwUV83UnJGcDBKNy1kZnZWLURDUWdybnZFNVgyYmJrRkhfQ1RZY2gyMmtnMkpTa3ZFa2NlSVVFUE1qSkt6WHFFWFNxNFFvTzFycjV2UjI2ZDVRRzczRzBKdHJNRkY1VEhDbmxwdXYwUklPeDJUYTlNX0xnZkZvSWlIR0wwZnRJbncwYVVZZHVqTEV5NHdSMUZZVGpDNm9vOXZ1MWdhMGFvMDNaWWc?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data