protiviti®
Global Business Consulting

Transformative role of AI in fraud detection

The evolving landscape of fraud

The rise of Artificial Intelligence (AI) has fundamentally transformed the landscape of fraud detection, presenting unprecedented challenges and opportunities for businesses across industries.

First, the challenges. There is no doubt AI has enabled nefarious activity on multiple fronts. Fraudsters leverage AI-powered tools to orchestrate a myriad of deceptive schemes, from forging identities with a blend of real and fabricated data, to executing large-scale phishing frauds and employing voice cloning to manipulate bank transactions. The emergence of generative AI models like ChatGPT has facilitated the creation of tailored phishing emails and malware, aggravating the prevalence of cybercrimes. Recent data bear this out. Australians reported losses of $851 million to scams in 2020, according to agencies such as Scamwatch, ReportCyber, IDCARE, the Australian Financial Crimes Exchange (AFCX), and the Australian Securities and Investments Commission (ASIC). This figure saw a significant increase during the COVID-19 pandemic, escalating to $1.8 billion in 2021 and further surging to a record $3.1 billion in 2022. The latest report from the Australian Competition and Consumer Commission (ACCC) reveals that Australians lost $1.3 billion to fraudulent investment schemes in 2023.

In this piece, we delve into the evolving role of AI in combating fraud, exploring its impact, applications, and the imperative for businesses to embrace this technology to safeguard their assets and reputations.

That is where the opportunities come in.

Leveraging AI for enhanced fraud detection

In response to the above challenges, Australian businesses are turning to AI-powered solutions to enhance their fraud detection efforts. Outlined below are a range of AI-powered fraud detection techniques that are reshaping the landscape of fraud prevention:

- Anomaly detection, a cornerstone of AI-powered fraud detection, scrutinises vast datasets to identify aberrations indicative of fraudulent activity. By leveraging machine learning algorithms, anomaly detection systems can adapt to evolving fraud patterns, discerning subtle anomalies that evade conventional detection methods.
- Natural Language Processing (NLP) can analyse vast textual data to uncover keywords or descriptions linked to fraudulent activities. However, it is important to remember that NLP relies heavily on the quality of the data it processes - inaccurate or insufficient data can undermine its effectiveness.
- Convolutional Neural Networks (CNN) and Biometric Liveness Detection are powerful tools against deepfakes and other sophisticated forms of visual or audio spoofing. They highlight how AI can process high-dimensional and complex media data to detect irregularities that might go unnoticed by human detection methods.
- Large Language Models like GPT-3 have begun aiding manual fraud review processes by extracting relevant information from policy documents, thereby expediting decision-making on potential fraud cases.
- Prescriptive analytics heralds a new frontier in fraud prevention, offering actionable insights derived from a synthesis of data analytics techniques. By harnessing the predictive capabilities of AI, businesses can anticipate and mitigate fraud risks.
- Synthetic data generation represents an innovative approach to training AI models. By creating artificial but statistically reflective examples of real-world scenarios, synthetic data offers a way to improve the variety and sophistication of examples used for training without violating privacy regulations or depleting limited datasets.

Australian financial institutions and organisations are actively investing in AI-driven fraud detection technologies, including AI-powered anomaly detection systems to identify and mitigate fraudulent activities more effectively. The Australian Federal Police (AFP) has started using AI to help identify potentially fraudulent activities and money laundering cases.

This use of AI offers significant opportunities for financial institutions to streamline their fraud prevention measures, reducing the need for extensive manpower. AI-driven analytics afford real-time transaction monitoring, proactive identification of potential fraud with reduced human errors, and collaborative defence through shared insights on emerging fraudulent strategies, enhancing adaptability and ensuring up-to-date regulatory compliance. Addressing the multifaceted challenges of fraud necessitates a collaborative approach, encompassing data sharing initiatives, regulatory reforms, and cross-sectoral partnerships. By fostering responsible data sharing practices and leveraging the latest advancements in cloud computing and AI, businesses can fortify their defences against fraud while upholding individual privacy rights.

As we navigate the complexities of the digital age, proactive adoption of AI represents a pivotal step towards ensuring financial security and resilience in the face of emerging threats.

How Protiviti can help

Protiviti's AI-driven solutions are designed to enhance the capabilities of organisations in detecting and preventing fraud. By implementing an AI-based system, one client experienced a notable decrease in the incidence of fraudulent transactions. The technology applied sophisticated machine learning techniques to discern anomalies within transaction data reliably. This improvement was not only instrumental in reducing financial losses but also served to optimise the accuracy of fraud detection processes, thereby lessening the occurrence of false positives. In a separate case involving an insurance company, Protiviti integrated natural language processing tools to scrutinise claim submissions. This led to an enhanced ability to detect discrepancies and potential signs of fraud within text-based data, resulting in a marked decline in fraudulent claims being paid out.

The strategic implementation of AI in fraud prevention not only streamlines processes but also presents a host of transformative opportunities. Primarily, AI significantly reduces operational costs by minimising the need for extensive manpower dedicated to monitoring and analysis tasks. This automation allows skilled personnel to focus on more strategic initiatives, enhancing overall productivity and innovation within financial institutions. The development and deployment of these technologies also consider regulatory compliance across different jurisdictions while providing improved security measures against various forms of fraud.

When integrating such systems, Protiviti emphasises maintaining data integrity and privacy standards alongside ensuring compatibility with existing infrastructure—all without diminishing the essential role humans play in oversight functions. Adopting AI-powered tools has provided our clients with stronger protection against complex fraudulent schemes as well as bolstered their efficiency in operations management; this alignment with strategic goals supports both immediate needs and long-term resilience against risks associated with fraudulent activities.

Contacts

Matthew Pirera
Managing Director
AML & financial crime lead
matthew.pirera@protiviti.com.au

Anthony Hodgkinson
Director
Fraud & forensics lead
anthony.hodgkinson@protiviti.com.au