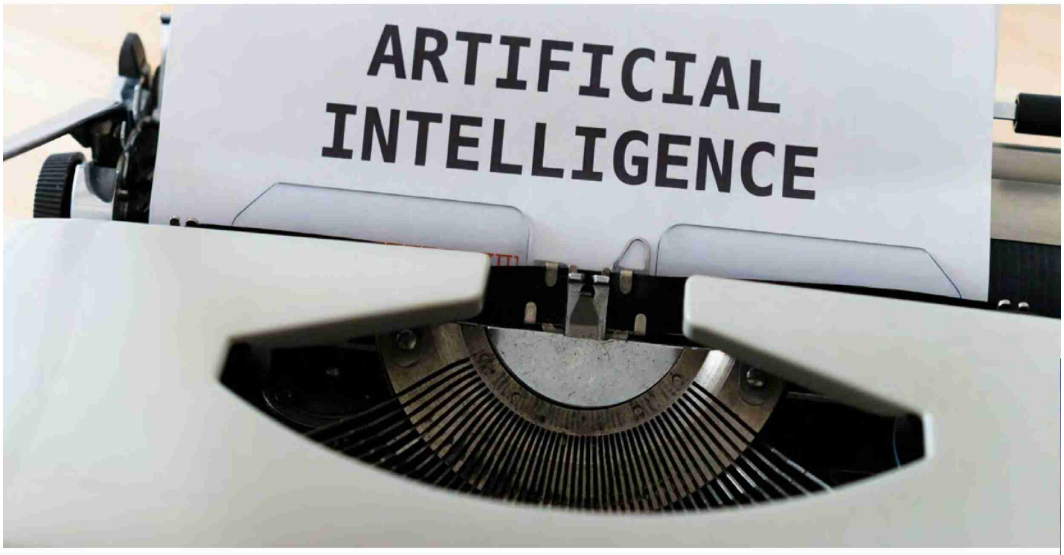
Publication: Premier
Title: The New Face of Fraud
AVE: 53553.15
Page: 32
Publish Date: 01 July 2026
Author: Unspecified

The New Face of Fraud

How AI is Becoming the Accomplice

Fraud is evolving at an unprecedented pace. For decades, corporate fraud followed relatively predictable patterns: manipulated invoices, unauthorised payments, falsified documents, and occasional insider misconduct. While these traditional threats persist, a far more sophisticated layer is now emerging – one that many organisations are only beginning to comprehend fully.



Artificial intelligence is fundamentally reshaping the fraud landscape. What once demanded extensive criminal networks, significant resources, and considerable time can now be executed quickly, inexpensively, and at scale. AI tools can generate highly convincing documents, clone voices with remarkable accuracy, and fabricate identities that appear legitimate at first glance. This technological shift is compelling businesses across sectors to urgently reassess their approaches to fraud detection, investigation, and prevention.

One of the most alarming trends is the surge in AI-enabled impersonation attacks. Internationally, fraudsters have increasingly used voice cloning technology to mimic senior executives, authorising large, time-sensitive payments that bypass normal scrutiny. In other instances, synthetic identities – blending real and fabricated personal data – have successfully navigated onboarding processes to establish seemingly genuine supplier accounts or employee profiles.

These tactics prey on a fundamental human and organisational vulnerability: trust. When a request appears to originate from a familiar voice, a verified email address, or an established business partner, employees and systems tend to respond swiftly without further question. Fraudsters understand this dynamic intimately, and AI now enables them to replicate those signals of legitimacy with disturbing precision.

EMERGING PATTERNS IN AI-ASSISTED FRAUD

The range of AI-powered techniques is expanding rapidly. Organisations are encountering:

- AI-generated documents crafted to support fraudulent transactions or streamline supplier onboarding, complete with realistic letterheads, signatures, and supporting metadata.
- Voice cloning is used to impersonate executives or finance leaders during urgent payment requests, often delivered via telephone or voicemail with a convincing emotional tone and speech patterns.
- Synthetic identities constructed from mixtures of real and fabricated data, designed to evade standard verification checks.
- AI-written communications that mimic an organisation's internal language, tone, and even specific jargon, making phishing emails or internal messages far harder to detect.

Publication: Premier
Title: The New Face of Fraud
AVE: 53553.15

Page: 32
Publish Date: 01 July 2026
Author: Unspecified

- Highly automated phishing campaigns that adapt in real time, producing content that is significantly more personalised and persuasive than traditional scams.

This sophistication raises a critical question for boards, risk leaders, and finance teams: how can organisations defend themselves against threats that can so convincingly imitate both people and established systems?

The answer lies in recognising that technology alone cannot provide a complete solution. True resilience emerges from the thoughtful integration of robust controls, heightened awareness, and professional investigative capability.

FIVE PRACTICAL STEPS TO STRENGTHEN DEFENCES AGAINST AI-ENABLED FRAUD

1 **Strengthen Verification Protocols** All high-value payments, supplier modifications, and sensitive requests should require secondary verification through an independent communication channel – such as a phone call to a known number or in-person confirmation. Relying solely on digital channels is no longer sufficient in an era of advanced impersonation.

2 **Implement Multi-Layer Approval Processes.** Critical financial transactions should never rest on a single individual's authority. Independent review mechanisms, including segregation of duties and escalation protocols for unusual requests, create essential safeguards that are harder for AI-assisted schemes to circumvent.

3 **Enhance Employee Training on AI-Driven Deception** Awareness programmes must evolve beyond basic phishing recognition. Regular training should incorporate real-world examples of voice cloning, deepfake videos, synthetic media, and sophisticated AI-generated correspondence. Employees at all levels, particularly those handling financial matters, need the skills to spot subtle anomalies.

4 **Adopt Advanced Digital Monitoring and Anomaly Detection.** Proactive monitoring of digital activity can identify unusual patterns – such as irregular login times, atypical email behaviours, or unexpected changes in supplier details – before they develop into full-scale incidents. Modern tools leveraging behavioural analytics play a vital role here.

5 **Build Forensic Readiness.** Organisations must prepare for the inevitable by establishing clear protocols for evidence preservation. When an incident occurs, the ability to rapidly secure digital artefacts, conduct thorough investigations, and present findings with credibility can make the difference between successful recovery and significant loss. Specialist forensic expertise is increasingly essential in this domain.

As technology continues to advance, fraud will undoubtedly evolve alongside it. The most resilient organisations will be those that move beyond viewing fraud prevention as merely a matter of policies and technical controls. Instead, they will recognise the complex intersection of technology, human behaviour, and governance.

In today's environment, the stakes extend far beyond financial loss. Fraud now targets information, identity, and trust – foundational elements of modern business operations. Protecting these assets demands a new level of forensic thinking and strategic vigilance.

Loxton Forensics continues to support organisations in navigating this challenging landscape through expert investigation, risk assessment, and tailored resilience strategies. By combining deep forensic capability with an understanding of emerging technological threats, businesses can not only respond effectively to incidents but also build stronger defences for the future.

The message is clear: those who treat AI-enabled fraud as a distant or secondary concern do so at their peril. Proactive adaptation is no longer optional – it is a business imperative.

Text by Loxton Forensics
Photography © Pexels.com