



STELLALANDER-VRYBURG: Fraud is evolving rapidly, with artificial intelligence (AI) emerging as a powerful tool for criminals and posing new challenges for businesses and organisations. According to Loxton Forensics, while traditional forms of corporate fraud, such as manipulated invoices, unauthorised payments and falsified documents, remain prevalent, a more sophisticated layer of AI-enabled deception is beginning to take hold.

Modern AI tools are capable of generating highly convincing documents, imitating human voices and creating realistic digital identities. This has significantly lowered the barrier to entry for fraud, allowing individuals or small groups to carry out complex schemes that previously required organised criminal networks. One of the most concerning developments is AI-enabled impersonation. Internationally, there have been cases where fraudsters used voice-cloning technology to mimic senior executives and authorise urgent payments. In other instances, so-called “synthetic identities” have been used to bypass verification processes or create fraudulent supplier accounts. These methods rely heavily on exploiting trust within organisations. Messages that appear to come from known colleagues, verified email addresses or legitimate suppliers are more likely to be acted on without question. Emerging trends identified by Loxton Forensics include AI-generated documents used to support fraudulent transactions, voice cloning in payment requests, and increasingly sophisticated phishing campaigns designed to mirror internal communication styles. Experts warn that defending

against such threats requires more than technology alone. A combination of strong internal controls, employee awareness and effective investigative processes is essential. Practical measures recommended to mitigate risk include stricter verification procedures for high-value transactions, multi-level approval systems, and enhanced monitoring of digital activity to detect unusual patterns. Employee training has also become increasingly important, particularly in recognising deepfake communication and advanced phishing attempts.

In addition, organisations are being encouraged to improve their forensic readiness, ensuring that digital evidence can be preserved and investigated efficiently in the event of suspected fraud. As AI continues to advance, experts say fraud prevention will depend on understanding the intersection between technology, human behaviour and governance. Loxton Forensics notes that modern fraud is no longer limited to financial loss, but also involves the manipulation of information, identity and trust, making vigilance and adaptability critical in an increasingly digital environment.

[Full Page Image](#)