Press Release

The war on financial fraud

Compliance made easy with digital technologies

By Sameer Kumandan, MD of SearchWorks360

The digital transformation of financial services has introduced unparalleled convenience, with mobile apps, QR payments, and online onboarding now the norm. But as South Africans embrace these innovations, a silent threat is growing in tandem: cyber-enabled financial fraud.

The increasing digitisation of banking and financial services has broadened the attack surface for criminals. From deepfake scams and business email compromise to ransomware and social engineering, fraud tactics are becoming more sophisticated – and more dangerous. Each digital interaction, if not properly secured, can become an entry point for exploitation.

A recent international case made headlines when an employee was tricked into paying $25.6 million to cyber scammers after joining a fake video conference call. The fraudsters used deepfake technology to convincingly impersonate the company's CFO, instructing the employee to process 15 payments – not realising she was the only human participant on the call.

"South Africa's compliance frameworks must evolve as fast as fraud tactics do," says Sameer Kumandan, Managing Director of SearchWorks360. "We can no longer afford to view compliance as a tick-box exercise. It must be technology-led, dynamic, and proactive."

A rapidly evolving threat landscape

Recent reports from SABRIC and the Financial Intelligence Centre confirm what many in the industry already know: financial fraud is on the rise, with cybercriminals increasingly exploiting weaknesses in both digital infrastructure and human behaviour. The FIC's latest sector risk assessment for crypto asset service providers highlights just how quickly fraud vectors are multiplying – especially in newer, less regulated financial arenas.

These developments have exposed gaps in the country's traditional compliance framework, which, while robust in its intent, is struggling to keep pace with a rapidly shifting digital finance environment.

South Africa's existing compliance landscape

South Africa already has several key laws and regulations aimed at combating financial crime, including the Financial Intelligence Centre Act (FICA), the Protection of Personal Information Act (POPIA), the Prevention of Organised Crime Act (POCA), the Financial Sector Regulation Act (FSRA), and AML/CFT standards aligned with FATF recommendations. These frameworks form the backbone of the country's efforts to prevent money laundering, data breaches, and cybercrime. However, many of these regulations were drafted before the rapid rise of digital finance, fintech startups, and decentralised transactions, and therefore require ongoing adaptation to remain effective.

The rise of RegTech: Compliance transformed

Regulatory Technology (RegTech) is now redefining how compliance is done. With tools like biometric verification, real-time identity checks, and AI-powered fraud detection, RegTech makes compliance faster, more accurate, and less prone to human error.

"Digital transformation isn't just helping institutions stay compliant, it's helping them become more resilient to financial crime," says Kumandan. Banks, insurers, and real estate agents use tools that verify customer IDs against Home Affairs data in seconds, automatically store FICA documents with full audit trails, and apply intelligent risk scoring that updates in real time.

By moving from reactive to proactive compliance, businesses can detect fraudulent activity in real time and stop losses before they occur. AI-driven analytics can surface complex fraud patterns that would go unnoticed by human teams, which is a critical capability in the current threat landscape.

Simplifying compliance with smart technology

VOCA, powered by SearchWorks, enables businesses to keep up with regulatory demands while simultaneously improving fraud detection capabilities. VOCA uses intelligent automation to continuously monitor client behaviour, flag risks early, and adapt to new compliance requirements.

By leveraging these technologies, financial institutions can reduce compliance gaps, avoid costly penalties, and strengthen their defences against an evolving threat landscape.

Ends