

Fraud trends indicate South Africa needs a proactive approach to turn the tide on financial malfeasance

Systemic vulnerabilities, cybercrime and social engineering add to pressures on institutions, businesses and the economy

Fraud in South Africa is on the rise with no signs of slowing. Amid an uptick in digital transformation across multiple sectors, cybercrime coupled with sophisticated social engineering techniques are laying bare systemic vulnerabilities in public institutions and businesses alike. In 2024, South Africa remained a global hotspot for fraud, [ranking](#) among the top five countries for cybercrime density.

“South Africa faces a perfect storm of fraud challenges that impact the entire breadth of the economy. From digital identity scams that affect consumers to complex procurement fraud that places organisations at risk, businesses need to adopt proactive strategies to mitigate financial and reputational damage as a matter of urgency,” notes Sameer Kumandan, Managing Director of [SearchWorks](#), an innovative data platform that allows users to conduct live, accurate searches on individuals and companies and in-depth KYC checks online.

A nation at risk

South Africa’s high fraud risk reflects the country’s adoption of digital technologies alongside clear gaps in combatting growing digital fraud. According to a [recent analysis](#) by TransUnion, 4.9% of digital transactions were flagged as suspicious in the first half of 2024. Telecommunications (8.0%), financial services (5.5%), and online communities (5.1%) are among the hardest hit as South Africa had the eighth highest rate of suspected digital fraud in the first half of 2024 out of the 19 countries where TransUnion provided regional breakdowns.

Identity fraud also spiked with synthetic identity scams (where personal data is manipulated to create false identities), which increased by an alarming 153% in just one year, according to TransUnion. In addition, the persistence of social engineering scams, including phishing, vishing, and SIM swap scams, has also contributed to the country’s fraud crisis. In 2023 alone, the South African Banking Risk Information Centre (SABRIC)

reported that phishing attacks cost South Africans an estimated R200 million, a 50% increase from the previous year.

Fraud within public institutions, including SASSA and Home Affairs, also highlight South Africa's vulnerability to fraud and cybercrime. Kumandan says the ongoing investigation into [R370 SRD grant fraud](#) and the exposure of [identity theft](#) at Home Affairs reveal underlying systemic issues and weaknesses that make it possible for fraudsters to operate undetected.

Factors driving fraud in 2024

"Trending fraud types like payment and procurement fraud, identity theft, and social engineering scams are often driven by a combination of cunning tactics by fraudsters and existing weaknesses within organisations. Legacy systems within organisations, human error, as well as a lack of tools or processes to identify fraud quickly create a cascade of challenges. Added to this are the advanced tools cyber attackers use, including AI-generated deepfakes to create convincing fake identities or bypass security measures," explains Kumandan.

Procurement fraud remains a pressing concern for organisations. According to the [PwC Global Economic Crime Survey](#), procurement fraud ranks among the top three economic crimes globally, with gaps in fraud detection systems leaving South African businesses particularly vulnerable. Fraud involving public institutions further complicates the picture. "Implementing appropriate checks and accurately verifying government suppliers and employees can help regulate processes and streamline operations to deliver much-needed critical services," says Kumandan.

Counting the cost of fraud

The Council for Scientific and Industrial Research (CSIR) estimates the impact of cybercrime on the South African economy to be at R2.2 billion per annum, with the country described as a 'very attractive' testbed for cybercriminals.

The repercussions of fraud extend far beyond financial losses, potential legal penalties and damaged brand reputations. "The consequences of inaction against fraud have an impact on the immediate victims as well as the broader economy. Overall trust in

organisations and public institutions is a critical ingredient in the functioning of a healthy society. The stakes are simply too high to ignore,” adds Kumandan.

Turning the tide through proactive prevention

At a broader level, taking a proactive stance against fraud is vital if South Africa wants to improve its economic position. To achieve this, Kumandan says it is necessary to strengthen good governance practices. “Having access to complete and accurate information on businesses and individuals, and the ability to verify credentials enables better, more transparent decision-making, which in turn can create greater trust between organisations and their stakeholders. Preventing and mitigating irregularities, fraud and corruption can through due diligence at all levels within organisations and public institutions.”

“By leveraging cutting-edge technologies and conducting thorough background checks, companies can protect their operations and ensure that fraudsters are kept at bay. SearchWorks provides the tools that organisations need to conduct these checks, ensuring compliance with relevant laws and mitigating risk,” he adds.

Ends.