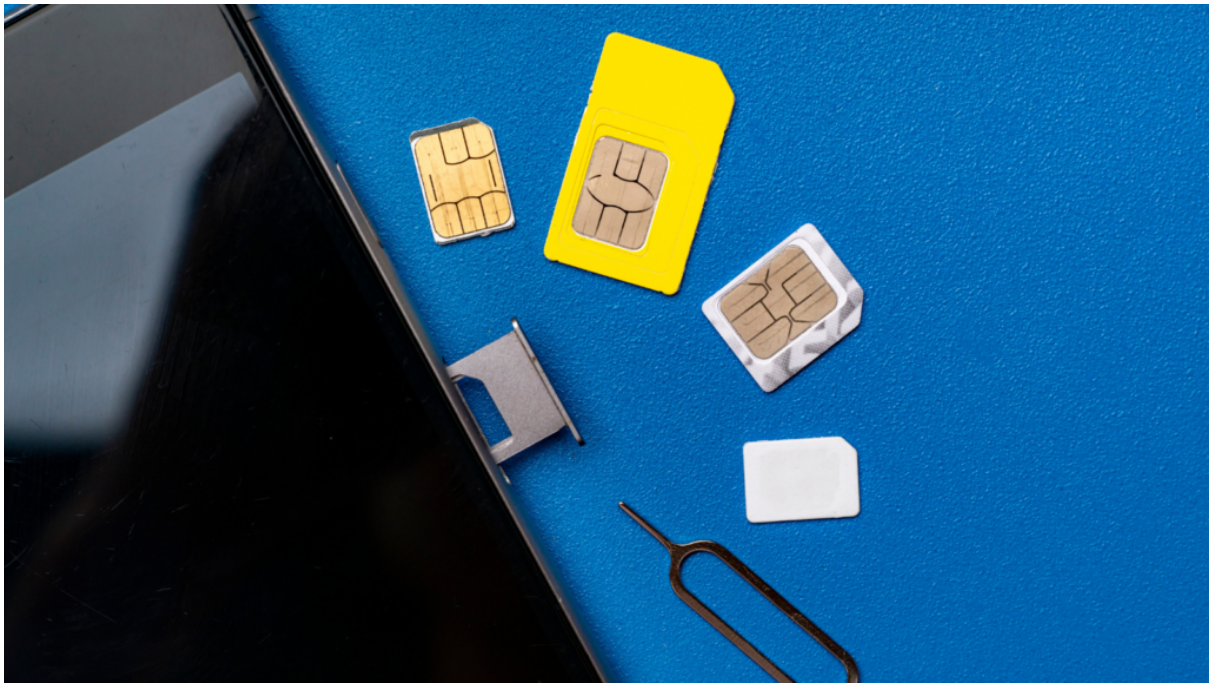
Warning to anyone with a smartphone in South Africa



South Africa loses R5.3 billion every year to telecommunications fraud, with nearly 60% of that linked to mobile banking fraud driven by SIM swaps.

“SIM swap fraud is the enabler that the criminals use to intercept a one-time password (OTP) to take over a social media account,” former Vodacom Chief Risk Officer Johan van Graan told Moneyweb Radio.

“The actual fraud is by accessing the internet banking where they have previously phished this PIN (personal identification number) and password of a customer, sending WhatsApp messages to say I need money.”

Van Graan said the actual fraud takes place outside the telecoms network, when fraudsters log in to banking applications and social media platforms.

He said that South Africans often share PINs and passwords, which helps criminals access personal information.

The current RICA Act (Regulation of Interception of Communications and Provision of Communication-Related Information), which applies to telecom networks, makes it difficult to authenticate the true customer or owner of a phone number during a SIM swap request.

“I propose facial recognition because it works in the banking sector for FICA (Financial Intelligence Centre Act). Then, when a SIM swap does take place, the networks must use that facial recognition to validate the SIM swap,” he said.

The Rica Act, which has been effective since the second half of 2005, is a law that aims to regulate the interception of communications by requiring the registration of all SIM cards.

The act requires that SIM card users provide proof of identity and proof of residential address when purchasing a SIM card to use for mobile services, which allows law enforcement to trace users.

The RICA Act requires people purchasing a SIM card to provide:

- Full names and ID number
- A certified copy of ID document
- Proof of residence (not older than three months)

Concerns over online privacy and safety

Van Graan highlighted several problems with the Rica process. He said the issue at hand is that the Rica Act has two main components.

The interception aspect, according to van Graan, is likely among the world’s top five most stringent, especially after recent changes affecting journalists and lawyers.

However, he said the customer registration process ranks among the bottom five globally.

According to the act, when a customer approaches a RICA agent, the agent checks the presented ID, matches it to the customer's face, and manually records the name, ID number or passport number, and address.

"There's no validation of the information. No copy of the IDs is kept. None of that information is kept," he said.

For postpaid customers, networks can conduct credit vetting to gather additional information and have the ability to use facial or biometric recognition.

However, the significant challenge is that 80% of South African customers use prepaid services, which means there is no reliable validation process during a SIM swap.

"The networks have the technology to enforce it, so pre-RICA SIMs will stop. Also, because the biometrics is needed at time of SIM swap, it will definitely, I would say 99% reduce SIM swap fraud," he said.

Van Graan said the issue lies with the regulator. When South Africa was placed on the FATF (Financial Action Task Force) grey list, this was one of the highlighted concerns.

He attended a meeting with the former Minister of Justice, Ronald Lamola, where he requested that the networks develop a solution.

The networks have complied by proposing a solution to the government through the Electronic Communications Act (ECA).

"I just think the logjam is that it's lying somewhere in the legislative change process. It's not important enough, or there aren't people who can rewrite the act."

The networks could embrace the change, as it should help minimise the washing machine effect, in which around 60% of prepaid SIM cards are recycled every year.