Home Affairs' biometric ID verification a big step towards curbing crime

While biometric identification is nothing new, Home Affairs' implementation of the Automated Biometric Identification System (ABIS) is a significant landmark in its capacity to provide a single data repository.

© nicoelnino – 123RF.com

"Automated Biometric Identification System is a milestone in South Africa's pathway towards a new digital national identity system," said Department of Home Affairs (DHA) Minister Malusi Gigaba, at the May 2018 launch.

As part of the capturing of biometrics, the DHA is also set to improve access to South Africa, with the roll-out of eVisas, with the pilot phase expected to begin in early-2019.

While the system will help to curb theft by biometric authentication requirement, says Manie van Schalkwyk, executive director Southern African Fraud (SAFPS), fingerprint identification has been available to banks for many years.

What is different with the system at Home Affairs is that it provides a centralised data source of consumer information. "This fingerprint identification is a cradle to grave situation," Van Schalkwyk says. "In other words, it will allow for enhanced

and safer data in terms of digital processing, storage of photos, fingerprints, signature, voice recording, demographic information and scanned supporting documents. Thus, it makes it easier to verify all the pieces of information pertaining to an individual."

There has been an increase in new fraud listings of 52% more this year than last year and identity theft is one of the most serious concerns. The request for Protection Registration is up by 70%, which is further indication of the real increase in fraud, Van Schalkwyk says.

"A biometric system definitely curbs fraud, but what consumers must be careful of is that when fraudsters are stopped in one way, they will get creative in another."

A common tactic, he says, "is to recruit runners, or money mules, as they are called in the United Kingdom, to open accounts in their own names that then become a biometric match for the fraudster and leaves the runner in a great deal of trouble."

There has also been a surge in online fraud where people are enticed by an email notification of a prize win, or the inheritance of a deceased rich uncle, which requests bank details for the funds to be transferred.

This also happens by phone, he adds. "A caller will phone posing as a legitimate bank employee with a story to 'authorise a debit order that is about to be processed on your account'. They will extract a lot of information from you and even go as far as asking for your password, admitting that they know they should not be asking for it. The money in your account will be wiped out. Once you have given your password willingly, you have no recourse with your bank," Van Schalkwyk cautions.

"Never provide information where you have not solicited the enquiry yourself," he adds. "We are in the electronic age where information is easily available to fraudsters. Treat your information in the same way that you treat cash. Be prudent."

If you feel your privacy has been threatened then it is advisable to apply for Protective Registration on the SAFPS website. This will provide added security and alert the credit provider or the bank that the specific ID number has been compromised. This service is free of charge to consumers.

Go to www.safps.org.za, click on lost passport/ID to apply for temporary Protective Registration that will be issued on line or SMS the word "protectid" to 43366.