

African Bank Ltd press release

6 July 2021

Protect your personal information from identity thieves

Identity theft is one of the fastest growing crimes in the world. Experts believe that someone's identity is stolen somewhere in the world every two seconds.

According to the SAFPS' 2020 statistics, there were significant increases in key areas, such as fraud listings that increased by 62%, victim listings increasing by 54% and impersonation fraud by 337%.

Impersonation fraud happens when a criminal impersonates you by stealing your identity and then opening credit accounts in your name such as vehicle finance, store credit or cellphone contracts.

African Bank's Chief Risk Officer Piet Swanepoel says despite this, most people believe it cannot happen to them until it does, and their credit worthiness has been destroyed.

Victims only become aware when they start to receive letters of demand for debts, they know nothing about, or when their own application for credit is refused because they have an unhealthy credit record.

Don't allow ID theft and fraud to go undetected. Check your credit report every month before the damage is done. With some banks, like African Bank you can even access a monthly credit report free of charge on internet banking or by downloading their banking app.

"You need to be able to detect, quickly, whether your identity has been compromised to enquire for credit or open new accounts before thieves run up huge debts in your name.

"When anyone applies for credit from a credit or service provider, an enquiry for credit made at a credit bureau will appear on that person's credit report. By regularly accessing a free credit report, you can take action before too much damage is done," he says.

Ways in which syndicates can steal your identity:

- ✓ By forging the documents which are needed to apply for credit in your name – fake identity documents, passports or driver's licences.
- ✓ Steal bank statements and proof of address from your mailbox or dustbin.
- ✓ Gain access to your online banking credentials or credit card details to perform online transactions in your name.
- ✓ SIM swaps to intercept One Time Pins sent to you while transacting online.
- ✓ Hack into online shopping platforms you've bought items on.
- ✓ Obtain information from your social media profiles.

Any document, printed or electronic, that contains your name and other personal information puts you at risk of identity theft, Swanepoel warns.

Steps consumers can take to better protect their personal information:

1. Keep all private correspondence private – lock your postbox, destroy old accounts with your personal details on them.
2. Create strong online passwords and different passwords for each account.
3. Regularly review your credit bureau profile for signs of suspicious activity.
4. Never disclose personal information such as passwords and PINs when asked to do so by anyone via telephone, fax, text messages or email.

If you find you have fallen victim to identity theft, these are the steps to take:

1. Report this to the police and the company, bank or financial institution where the fraud occurred. SAPS should provide a case number and the institution a ticket and/or reference number.
2. If a bank account has been fraudulently opened using your identity, close your existing bank accounts and the bank accounts opened by the thief. Request new accounts and PINs. Depending on the type of fraud, make sure you are dealing with the bank directly and not an interloper.
3. You will be required to provide information that proves that you did not enter into the relevant financial agreement yourself.
4. If a cell handset was stolen, report it to your service provider to blacklist the phone, and confirm your number was not targeted in a sim-swap to intercept one-time pins.
5. Apply for a free Protective Registration listing with Southern Africa Fraud Prevention Service (SAFPS). This service alerts SAFPS members, which includes banks and credit providers that additional care needs to be taken to confirm that they are transacting with the legitimate identity holder. Consumers wanting to apply for a Protective Registration can visit the SAFPS website (<http://www.safps.org.za>) and “Register Now”.
6. If the credit provider is a SAFPS member, a victim of impersonation filing and/or Protective Registration will be loaded on to SAFPS database on your behalf. Once you have established your innocence, the credit provider will issue you a letter confirming that you have been the victim of impersonation.

“Identity theft is rife across the world. The uptake in the use of mobile devices and online transacting has created even more means for thieves to con people out of their hard-earned money or steal their identity to commit fraud,” Swanepoel concludes.

“It is up to consumers to take the lead and put in the place the necessary means to protect their personal information. The key is to be vigilant at all times and to react immediately to notifications of transactions which are suspicious.”

ENDS

Visit the African Bank [website](#) or like them on [Facebook](#), [Twitter](#) and [LinkedIn](#)

PREPARED ON BEHALF OF AFRICAN BANK BY CATHY FINDLEY PR. CONTACT JACQUI MOLOI ON JACQUI@FINDLEYPR.CO.ZA OR 071 7648233 WITH ANY CONSUMER PR QUERIES.