African Bank Limited Press Release

March 2017

How card savvy are you?

Stolen-card, counterfeit-card and card-not-present (CNP) fraud are the three most prevalent types of fraud used to defraud customers.

African Bank's Alfred Ramosedi, Sales and Marketing Executive, says criminals are getting more and more sophisticated in their fraud scams but the three modus operandi listed above are still the most prevalent and consumers should familiarise themselves with these scams and the means to protect themselves.

"Stolen-card fraud is pretty self-explanatory," says Ramosedi. "Criminals steal genuine bank cards together with the correct pin numbers and then use these cards immediately at the nearest ATM to withdraw cash followed by purchases at stores until the account is either empty or the card stopped."

Counterfeit-card fraud is slightly different in that a card is manufactured fraudulently and not genuinely issued by a bank. Criminals can do this by using compromised card data. The data is usually compromised through skimming. Ramosedi says skimming devices can read and store card data on the magnetic strip of a genuinely issued bank card. "The problem is hand-held skimming devices are quite small and are not easily detectible. ATM skimming devices are fixed onto the machines and are even more difficult to see so criminals often get away with skimming undetected," says Ramosedi. Although these counterfeit cards can only be used at an ATM if the correct pin is also used, most criminals generally manage to view the pin with a technique called shoulder surfing. "Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a pin number at an ATM machine, or use a calling card at a public pay phone."

Finally with CNP fraud, the data is compromised in a variety of ways. Ramosedi says this can range from the actual physical theft of data off a genuine card to large scale data breaches usually carried out by syndicates. While it may be difficult for a consumer to avoid a large-scale breach, they can do much to mitigate the risk of the low tech physical theft. "Many people do not even realise that a criminal who can memorise or write down the card number of their card, its expiry date and the three digits on the back of the bank card, can quite effectively start transacting fraudulently on the internet or phone just as if they were the genuine card holder."

Similarly if a merchant has copies recording the front and back of various bank cards, these can be stolen and used fraudulently.

Ramosedi provides card holders with the following useful tips to protect their card data:

Tips for card holders:

- ✓ Review your account statements on a regular and timely basis; query any suspicious or unfamiliar transactions with your bank immediately.
- ✓ When shopping online, only place orders with your card on secure websites.
- ✓ Do not send e-mails that quote your card number and expiry date.
- ✓ Ensure that you get your own card back after every purchase and always ask that the credit card machine is swiped in front of you.
- ✓ Never write down your pin or disclose it to anyone.
- ✓ Report lost and stolen cards immediately to your bank
- ✓ Destroy your credit card receipts before discarding them.
- ✓ Sign your card on the back signature panel as soon as you receive it to stop anyone else from taking ownership or trying to use it.
- ✓ Don't allow anyone to use your card, your credit/debit card is not transferable. Only the person to whom the card was issued is authorised to use it.
- ✓ If you have a debit, cheque and credit card, don't choose the same pin for all of them, so that if your pin is compromised on one card, the others will still be safe.
- ✓ Always check transaction slips for correct purchase amounts before you sign them.
- ✓ Keep your transaction slips and check them against your statement to spot any suspicious transactions and query them immediately.
- ✓ Make a list of all your cards and their numbers and store it in a safe place.
- ✓ While transacting always keep an eye on the ATM card slot to ensure that your card is not taken out, skimmed and replaced without your knowledge.
- ✓ Should an ATM retain your card, contact your bank and block your card before you leave the ATM.
- ✓ Subscribe to your bank's SMS notification services; this will inform you of any transactional activity on your account.
- ✓ Save your bank's phone number on your phone for easy access in case of emergency
- ✓ Do not use an easy PIN number and avoid obvious choices like birth dates and first names.

Ends

Visit the African Bank website or like them on Facebook

PREPARED ON BEHALF OF AFRICAN BANK BY CATHY FINDLEY PR. CONTACT JACQUI RORKE ON JACQUI@FINDLEYPR.CO.ZA OR (011) 463-6372 WITH ANY CONSUMER PR QUERIES.