MEDIA RELEASE

FOR IMMEDIATE RELEASE APRIL 2021

Press Release: Protect your livelihood-Do not Take the Bait: A Warning from the OBS

With an increase in banking fraud, and a modus operandi of targeting online transactions, banks are continuing to evolve their products, services and systems to try and stay ahead of fraudsters. This is being achieved through the development and introduction of world-class security systems and technologies which will aim to protect consumers from becoming potential fraud victims.

However, the banks are sadly unable to fully protect consumers from falling prey to the tactics used by fraudsters to obtain confidential information such as banking details, card information and one-time-pins (OTPs).

Despite numerous (regular) warnings regarding this from the banks, the South African Banking Risk Information ("SABRIC"), and numerous media based messages (TV, Radio, online publications and interviews) by the Ombudsman for Banking Services (OBS), the OBS continues to receive complaints on a daily basis from consumers' who were deceived into providing the confidential banking information to fraudsters. "Just a couple of years ago, the most common scam was the phishing emails. This seems to have been overtaken by vishing scams (the fraudulent phone calls)," says Reana Steyn, Banking Ombudsman. In just these past few months, the OBS recorded more than 640. new fraud complaints that were received despite the daily warnings about these scams.

Targeting the most vulnerable

“What is very clear from the cases that have been received and investigated by the OBS is that anyone and everyone can be a target. However, the devastation caused by these scams to elderly citizens and pensioners (some of the most vulnerable members of society), is beyond heart-breaking,” says Steyn. She added that in many of these cases, it is not possible to recover any of the funds which have disappeared. The result of this is that an already vulnerable group of people are left without any recourse. “This often leads to destitution. While this fraud may be crippling to a person who is working, at least they have an opportunity to rebuild their savings. We have had cases where an elderly person’s entire pension is stolen due to the fraud and there is no way, or time, for an 80-year-old pensioner to make up the loss,” says Steyn.

Unless the money is stolen at the bank or lost through the fault of an employee or a technological glitch at the bank, it is ultimately up to consumers to do all they can to protect themselves by staying informed about banking scams. The OBS again urges consumers to always be very critical about the person at the other end of the line asking for personal details to be shared. If in doubt, go to or call your nearest branch and speak to a consultant who will clarify the request for you if it is legitimate.

Covid game changer

The Covid-19 Pandemic has been a major global disrupter. Statistics show that in many markets around the world, consumers are prioritizing their health and safety over their need to conduct physical transaction, be it purchasing groceries or transacting at their bank. This trend has been replicated in the South African market to a large extent.

“With the exponential rise in online transactions as opposed to in-branch transactions, vishing scams have become one of the preferred methods for fraudsters to steal bank customer’s money. It must be pointed out that these individuals are very believable and are so convincing that consumers are lulled into a false sense of validity (that the request is legitimate) which then leads to the fraud taking place,” says Steyn.

How the scam works:

- A bank customer will receive a phone call from someone who says they are from the customer's bank;
- The customer is informed that funds have been fraudulently taken from their account or that they (the bank representative) is helping the customer to claim from a rewards program that is offered by the bank. For this to take place, the customer needs to confirm their details so that the funds can be credited to their account;
- Alternatively, customers are told that they need to act quickly and urgently, as fraudsters "*are about to take funds out of their account, but this can be stopped, if they act quickly and do-operate*"!
- The fraudster already has the customer's phone number (he/she is calling the customer) and may have a host of other personal information at his/her fingertips. This includes addresses, ID numbers, other contact details, email addresses, employment details, or NB even a customer's bank card number;
- The customer is asked to update or verify their details, possibly on their cell phone;
- The customer is then requested to provide everything required to access their bank account, such as card details, the cards pin number, transaction OTPs, and mobile or internet banking passwords. The fraudster says that this is necessary for them to assist the customer, to redeem the rewards, to do a transaction, stop a fraudulent payment, or recover the *stolen money*;.
- Once the customer has provided the requested details, their accounts are emptied.

The possible stories behind these scams are endless. The following case studies demonstrate the typical modus operandi of the fraudsters. The actual names of the victims have been altered:

#Pensioners being tricked – more than once. Mr X, is a 69 year old pensioner who received a call from a person (fraudster) who claimed that they were from the bank. He was advised that the bank was in the process of stopping unlawful transactions that had been made from his account. The fraudster requested the OTP that had been sent by the bank which he gave them. An amount

of R10 000was stolen from his account. He complained to the OBS. In this instance, despite being 100% at fault for the loss, the bank considered him a vulnerable consumer. As a gesture of goodwill, the bank gave him a full refunded and educated him about the various types of fraud. The bank further assisted him with downloading the bank's app on his phone to improve the security measures in place to prevent this type of incident. A few months later, he received a call from fraudsters and was persuaded into processing a transaction of R26 500from his banking app. He reported the matter to the bank and his profile was blocked. He received another call from the fraudsters a month later and again disclosed his confidential banking details resulting in R5 500.00 being stolen from his account. While the bank declined to refund the R26 500, through the OBS's investigation, it was discovered that the last transaction should not have been successful as his profile was supposed to be blocked. The bank agreed to refund the full amount of the last fraudulent transaction (R5 500).

"We need to stress the fact that the fraudsters are extremely sophisticated and convincing con-artists. It will be foolish to think that you will immediately see through the scam unless you are 100% clued up on these matters," says Steyn.

Pensioner act on investment advice from "her banker". Mrs Y, a 90-year-old pensioner, received a call from a fraudster who said that they were calling from her bank's fraud department. The fraudster provided her with his landline number and a reference number for the call. The fraudster also knew her e-mail address and these few seemingly unimportant facts put her mind at ease. The fraudster convinced her into investing in a product called Luno and the fraudster persuaded Mrs Y into purchasing Bitcoins. Since the complainant was convinced that she was talking to someone from the bank, she provided the fraudster with her ID number and proof of residence (documents that are required to register an account at Luno). When the fraud was discovered, an amount of R50 000 had been transferred from her bank account to a Luno account, and the funds were converted into Bitcoin. Unfortunately, no recovery was possible. Upon investigation of the matter, it transpired that she had given the fraudsters remote access to her computer. As such, her online banking details were compromised when she logged onto her online banking profile.

"As stated before, this type of scam is not only targeting pensioners, but anyone and everyone who engages with the fraudsters and believes their stories," stressed Steyn.

Social engineering fraud knows no boundaries. Mr Z described the following scenario that happened to him during lockdown last year. During the lockdown, he was unable to go to the shops to pay a clothing account. As a result, his account fell into arrears. He then received a call from someone claiming to be a representative of the clothing store and offered to assist him with settling his arrears through an online payment. The caller knew his name, his account number, and the fact that his account was in arrears. This put Mr Z at ease that the caller was a representative from the clothing store. The caller requested Mr Z to share his card number to allegedly "facilitate an online payment". Mr Z obliged. The caller then requested Mr Z to confirm the three-digit CVV number (PIN for online transactions) which was found on the back of his bank card. At this point, Mr Z became suspicious, hung up the call, and immediately contacted his bank's fraud department to report the incident.

"The lesson for all of us from these case studies is that criminals are smart. If we are ever going to make headway against these fraudsters, we need to become smarter," says Steyn. She added that consumers need to be alert to the various types of banking scams that are out there and teach themselves, their families, and communities, about the scams as well as the many safeguards provided by banks to prevent them from falling victim.

OBS tips on how to protect yourself from a vishing scam:

- Be aware. Always remember that legitimate businesses, especially Banks, will never ask you for your personal, sensitive, or confidential banking information (Pin, OTP, Password). Anyone who does this over the phone is probably a fraudster;
- Do not give in to pressure. If someone tries to coerce and/or pressurize you into giving them sensitive information hang up and immediately contact your bank's fraud department to report the incident. Especially if the prompt is of an urgent nature;
- Stay calm and do not panic. These criminals frequently play on unsuspecting consumer's emotions. Keep a cool head and hang up the phone. Call your bank, credit card company,

or wherever the caller claimed to be from immediately and verify whether there is a real problem;

- Always be sceptical. Even if your Caller ID gives the name of a bank, or some other company or organisation, it could be a trick;
- If you lose cellphone connectivity for some time for no apparent reason, receive an SMS for a Sim swap or a number port you did not request, contact your bank and then your network service provider immediately.

ENDS

How to get help from the Ombudsman for Banking Services during the lockdown.

The OBS has taken stringent measures to protect both our employees and complainants.

During lockdown, the OBS staff will be working remotely from home. However, the office is fully operational from 8am to 16:30pm, on Mondays and Wednesdays. When the office is closed, complainants cannot visit the OBS premises.

OBS staff are available to assist with enquiries and we encourage complainants to log complaints through our online and telephonic services. Complainants can lodge a complaint in one of the following ways:

o Online submissions (https://www.obssa.co.za/resolving-complaints/make-a-complaint/);

o By email: info@obssa.co.za;

o By phone: 0860 800 900;

o By WhatsApp: 066 473 0157

o By downloading an application form from the website., (https://www.obssa.co.za/wp-content/uploads/2018/04/Application-for-Assistance-form-FINAL.pdf)

Complainants who have already lodged a complaint may track their complaint online by clicking on the following link: https://www.obssa.co.za/track-a-complaint/. Alternatively, they can call the office to speak to our staff on 0860 800 900.

How to complain

"It is important that the proper protocol is followed when lodging a complaint. A formal, written complaint can be lodged directly with your bank's dispute resolution department. During this process, it is important to ask for a complaint reference number from your bank. Complainants also need to allow the bank 20 working days in to respond to your complaint. Finally, complainants need to obtain a written response from their bank," says Steyn.

Alternatively, consumers can contact the office of the Ombudsman for Banking Services for free assistance if they experience any banking problems or would like us to assist them with lodging a complaint against their bank.