Our ref: 201605-0007383

**Summary of the complaint**

The supplier permitted an illegal swapping of the complainant's cell phone sim card. This resulted in unknown persons being able to hack into his private banking accounts and stealing R144,000.00.

The complainant wants the supplier and his bank to take liability for his loss.

**Summary of THE SUPPLIER's response**

The supplier advised that it played no part in the compromising of the complainant's personal information that has resulted his bank account being accessed.

In order for an individual to access Online or Telephone banking platforms the said user would need to have ones: username/password/ card or account number/ internet banking pin, none of which is available through the supplier.

Therefore, the supplier accept no liability with regards to banking fraud, as it is not caused by any action or serviced by the supplier.

**Assessment**

We have considered all the evidence presented by both the complainant and the supplier and advise as follows:

It seems the complainant has been a victim of phishing fraud which resulted in a loss of R144 000.00.

**Phishing scams**

Phishing fraud involves fraudulent e-mails sent to unsuspecting bank customers in an effort to extract the customers' confidential internet banking credentials from them. The e-mail addresses used by the fraudsters often seem genuine, as the sender address implies that it was sent from a legitimate financial institution, whilst it is not.

The way the fraudsters phrase the e-mail content is an attempt to try to lure the reader into providing confidential information on the spot either by replying or by means of including links to a site that encourages the customer to disclose his/her bank account number, Personal Identification Number (PIN) and password and also randomly generated once-off passwords.

Fraudsters usually don't know where a specific individual or company banks. They send large volumes of e-mails randomly and by chance they are successful in targeting certain banks' customers.

If the reader responds to such an e-mail by entering or clicks on the link provided in the e-mail, a pop-up window will appear requesting him to enter one's confidential internet banking access details. This window usually appears to be the bank's legitimate website but it is not.

The fraudster can view the information entered on the false website, which he then uses to access the bank's genuine internet banking website and giving him/her access to the specific customer's internet banking profile.

Unfortunately, our office cannot assist in the investigation of this aspect of your matter. You can contact the Ombudsman for Banking Services for further assistance:

*Ombudsman for Banking Services*
Tel: 011-712-1800
Sharecall: 0860 800 800
E-mail us at: info@obssa.co.za
Web address: www.obssa.co.za

**SIM swapping**

In some instances, the fraudster in addition to the phishing attack itself, also performs a SIM swap in order to intercept the randomly generated once-off passwords.

SIM swapping is the process by means of which an individual (in this case the fraudster) approaches a cellular phone network provider for the issuing of a replacement SIM card on a particular cellular phone number. The applicant usually will argue that he/she lost his/her SIM card or that it was damaged.

Once a replacement SIM card is issued, the bank customer's existing SIM card will no longer function. The newly issued SIM card replaces the one in the bank customer's possession and therefore, all future communication would be directed to the replacement SIM card, including communication from the bank, more specifically the randomly generated once-off passwords.

In swapping an existing SIM card with a newly issued replacement SIM card, the fraudsters are able to intercept the randomly generated once-off passwords required to complete certain sensitive internet banking transactions.

As far as the cell phone service provider's liability in this regard is concerned kindly note that this matter has been considered in: *Nashua Mobile (Pty) Ltd v GC Pale CC t/a Invasive Plant Solutions 2012 (1) SA 615*

This case explores whether a plaintiff who alleges a contractual relationship with the defendant in the pleadings can permissibly sue the defendant in delict for losses arising from the defendant's failure to exercise due care in terms of the contract. Specifically, can a cell-phone client sue in delict a cell-phone service provider with which he has a contract for losses suffered by him following the negligent issue of a duplicate SIM card by the cell-phone service provider to a fraudster who then uses it to perform fraudulent internet banking transactions on his bank account?

As regards the causal link between the plaintiff's loss on the one hand and the defendant's negligent omission on the other, the court found that on the evidence of the plaintiff's own witnesses the defendant's negligent conduct in granting a duplicate SIM card to the fraudster without verifying his identity could not, on its own, have enabled the fraudster to access the plaintiff's internet bank account.

As there was no evidence that the other pieces of the puzzle required to access the plaintiff's internet bank account were negligently provided by the defendant, no liability could be imputed to the defendant in delict.

**Conclusion**

As per the decision in *Nashua Mobile (Pty) Ltd v GC Pale CC t/a Invasive Plant* Solutions the court concluded that the disclosure of the plaintiff's banking details was the ultimate cause of the loss suffered and that the cell phone service provider are therefore not liable.

Based on the precedent set in the above matter our office cannot instruct the supplier to compensate the complainant for the losses suffered.

Based on the facts of this case, the information and evidence furnished to this office and on the principles of reasonableness and fairness, there is no reasonable prospect of this office making a recommendation in the complainant's favour.

We regret that we cannot be of assistance and confirm that our file has been closed.

The complainant is advised that he may now take such other steps as he wish or refer the complaint to the National Consumer Commission in accordance with section 71:

71. (1) Any person may file a complaint concerning a matter contemplated in section
69 (1)(c)(ii) or (2)(b) with the Commission in the prescribed manner and form, alleging that a person has acted in a manner inconsistent with this Act.

The Commission may be contacted at:

Tel. 012 940 4500
Email: complaints@ncc.org.za; complaints@thencc.org.za;ncc@thedti.gov.za