ombudsman for banking services
SOUTH AFRICA

Consumer Note 8

Internet Banking Fraud

Please note that the information provided herein does not constitute expert legal, financial or technical advice. You should consult a relevant professional legal, financial or technical adviser for expert advice.

The purpose of the document is to provide you with practical information based on our experience. Each case we investigate is however assessed on its merits.

Background

Many bank customers successfully use electronic banking facilities such as internet banking but as with any other type of banking facility, they are also exposed to fraud and to various. The purpose of this note is to describe the diverse types of scams we are aware of and how we would approach a complaint of this nature.

The Code of Banking Practice

The Code of Banking Practice (hereafter "the Code") contains the following clauses relating to electronic banking facilities and more specifically, internet banking:

4. Our key commitments

We, the members of The Banking Association South Africa, undertake that we will act fairly and reasonably in a consistent and ethical manner toward you.

We undertake to:

4.5 provide reliable banking and payment systems services and take reasonable care to make these services safe and secure; …

9.3 Internet, telephone and cell phone banking

Internet, telephone and cell phone banking services make some banking services and transactions more easily accessible. However, as with all our products, there are certain precautions that you need to take to protect yourself against fraudulent transactions. Ensure that you familiarize yourself with these on our website or Internet banking portal, or with our telephone or cell phone banking departments.

We will take reasonable measures to ensure that our internet banking systems and technology are secure and are regularly reviewed and updated for this purpose. We will further:

9.3.1 provide you with regularly updated information on how to access internet banking services, including details about your customer ID, selection of appropriate passwords and the availability of additional authentication or security options, how to maintain your security and what your liability for unauthorised transactions will be;

9.3.2 inform you of the applicable Terms and Conditions relating to the use of internet banking services, including any fees and charges;

9.3. advise you of the current transaction limits that apply to our internet banking services. These limits may change from time to time and are available upon request;

9.3.4 inform you of what procedures you must follow to report unauthorised access to your information, accounts or disputed transactions using your internet banking service and provide you with effective and convenient means to notify us of security incidents and easily accessible contact points to report such activity as soon as you are aware of it; and

9.3.5 ensure that transactions of our e-banking services can be traced and checked as long as they are received by our systems.

In order to protect yourself from unauthorised electronic access to your accounts, please ensure that you:

9.3.6 review your statements and reconcile your accounts regularly;

9.3.7 change your temporary password to a password of your choice known only to you. Failure to change this temporary password immediately may be construed by the bank as negligence by you.

Do not under any circumstances reveal your secret access code/ PIN/password or other unique means of personal identification to anyone, and especially not to one of our staff members, as this can be used to access your electronic banking facility. Change any of these if you believe that someone may know your secret access code/ PIN/password or other unique means of personal identification;

9.3.8 do not use the browser facility to store your password in order to avoid having to enter it each time you transact using Internet banking;

9.3.9 rather type in our Internet address when logging in; do not use a link, ensure that the website is ours and not a fraudulent site and check the site security certificate for the Internet banking site each time before you do your banking;

9.3.10 *do not use computer terminals to which members of the public generally have access;*

9.3.11 *install and enable adequate anti-virus and security software on the computer you use for Internet banking. Do not leave your computer unattended when you are logged into your internet banking site;*

9.3.12 *treat emails, SMSs or calls you receive with caution and be aware that we will never ask you to reveal any personal account or security details (like your PIN, password, etc) in a letter, email, SMS or telephone call;*

9.3.13 *take care when entering numbers while doing your banking and in particular with telephone and cell phone banking so that when you make payments, you transfer the correct amounts to the correct accounts or beneficiaries. We cannot reverse duplicate or erroneous payments you make to other accounts without the specific consent of those account holders;*

9.3.14 *follow our advice - our websites are usually a good place to get help and guidance on how to stay safe online;*

Several types of internet banking fraud are known to occur:

Phishing scams

Phishing fraud involves sending fraudulent emails to unsuspecting bank customers to obtain the customers their confidential internet banking access codes and passwords. The email addresses used by the fraudsters often seem genuine, as they imply that the email was sent from a legitimate financial institution, whereas in fact it was not.

The way the fraudsters phrase the email is an attempt to lure the recipient into providing confidential information on the spot either by replying or by means of clicking on a link to a site that encourages the customer to disclose his/her bank account number, Personal Identification Number (PIN) and password, as well as their and randomly generated once-off passwords (OTPs) or random verification numbers (RVNs)

One of the ways fraudsters get hold of banking customers' email addresses is by means of the generation of a large volume of random combinations of names and domain addresses (for example absamail.co.za, hotmail.com, mweb.co.za, etc) on a trial and error basis to produce potential addresses for emailing.

Fraudsters usually don't know where a specific individual or company banks. They send large volumes of emails randomly in the hope of successfully targeting bank customers.

If the recipient responds to such an email by entering or clicks on the link provided in the email, a pop-up window will appear requesting him/her to enter his/her 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, giving him/her access to the specific customer's internet banking profile. Important to note is that the bank's internet banking website is not hacked into at any stage – the fraudster uses the information provided by an unsuspecting customer to enter the customer's legitimate internet banking profile.

Once access is gained to a customer's internet banking profile the fraudster will, for example, request to load a new beneficiary. This will then trigger a randomly generated once-off password (OTP/RVN) which is sent to the customer's cell phone. The customer, unknowingly, enters this randomly generated once-off password (OTP/RVN) as well, thereby disclosing it to the fraudsters. In some instances, the randomly generated once-off passwords are intercepted by means of a SIM swap being performed on the customer's cellular phone account. Such passwords are required to complete certain sensitive internet banking transactions e.g. creating new beneficiaries or increasing transfer limits.

The fraudster transfers the money to various accounts he or his accomplices have opened previously or have obtained access to. These accounts can be opened or used in various ways. By using fraudulent identity documents and forged residential information, by "purchasing" or "renting" accounts from unsuspecting account holders or by stealing legitimate ATM cards.

The fraudster generally uses a number of "runners" who immediately run to an ATM and make withdrawals from the accounts as soon as the money is transferred.

There are various variations to this type of internet banking fraud and thus the specific details may vary from incident to incident.

SIM swapping

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

SIM swapping is the process by 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 (OTP/RVN).

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

Key logging related fraud

There are two types of key loggers - software and hardware. The purpose thereof is to log all the keystrokes entered on a particular computer. The keystrokes are then retrieved by the fraudsters and used for their own purposes to access a customer's internet banking profile in that the confidential access information is retrieved in this manner.

Software key loggers

A software key logger, once installed on a computer, copies all keystrokes made by the user. Details of the keystrokes are saved to a file on the computer's hard drive where it can be retrieved by the attacker by means of hacking into the computer. In some cases, the key logger will send the file to the attacker's anonymous email address.

How is it installed?

This is done by hacking into the computer, installing the software on the physical machine or encouraging one to run an email attachment that, when executed, will install the key logger.

Hardware key loggers

Hardware key loggers are units that are usually installed within the keyboard or its cable. It also logs the user's keystrokes and stores them within the hardware unit. The attacker will retrieve the unit to access the keystrokes stored in it. Hardware key loggers can look like common computer equipment.

How is it installed?

The attacker needs physical access to your computer so that he can replace the keyboard and cable with one containing the keystroke logger.

A key logger can capture the user's card number, double lock password and PIN. Experience has furthermore shown that although the compromise takes place on a specific date, the actual attack may in some instances only occur months afterwards, the reason being that the fraudsters must unravel the keystrokes captured to use them in the correct order for purposes of entering the correct card number, double lock password and PIN. In addition, the fraudsters will experiment with the information obtained before the actual fraud is perpetrated – the fraudsters will monitor the accounts closely in order to see what the cash flow situation is, the available limits have to be established, the victim's specific security profile has to be determined (what types of transactions require randomly generated once-off passwords (OTP/RVN), how these passwords are dispatched, how the fraudster can intercept these passwords, etc). Should the fraudster not have a clear understanding of the specific internet banking profile, activity on the account could alert the victim in which case the victim will respond immediately by cancelling the card and the fraudster will have to start the process all over again.

Internal bank fraud

The public often believe that fraudsters can access the bank's internal computer systems to access bank accounts. While we cannot say that this is impossible, we are not aware of an instance locally or internationally where this has happened. Should this, however, happen a bank may either reject being vicariously liable for the actions of its staff member/s or may decide to settle a claim on reputational grounds. Based on our experience fraudsters will try to use the easiest method of accessing accounts and this is usually through the unsuspecting banking customer willingly supplying the information as discussed above.

Ombudsman's approach

When investigating internet banking fraud claims there are several aspects that we evaluate:

Access to the account information
We will first try to determine how the customer's confidential internet banking access information was compromised.

The banks can produce records of which internet provider address (IP address) was used to access the customer's internet banking profile when the fraud took place. The address is often the same as the address used in other similar fraud cases. In addition, the bank will also provide evidence as to an OTP/RVN being sent to the registered delivery method, usually a cellular phone number belonging to the customer. Proof of successful

delivery of the OTP/RVN to the customer's cellular phone together with proof of a different IP address being active on the customer's internet banking profile during the same time period will on a balance of probabilities be indicative that the customer divulged not only the confidential internet banking access information but also the OTP/RVN. In the absence of evidence of the bank's system being hacked into or any involvement by the bank in the scam, this will be the only reasonable conclusion we could come to, as we are not aware of any other means by which a fraudster would have been able to access the customer's account. Experience has also shown that fraudsters will sometimes change the OTP/RVN delivery destination so that all future generated OTPs/RVNs to be sent directly to the fraudster.

The banks will sometimes find evidence of the phishing email that was received on the customer's computer. The information will show that the email was received and the false website was accessed. We, however, do not require banks to perform forensic analysis on customers' computers – firstly, such analysis has to be done immediately before the evidence could possibly be corrupted, secondly such an intervention is very expensive and lastly the alternative evidence available is sufficient to come to a finding in cases of this nature. In some instances, customers will admit to divulging their confidential internet banking access details by responding to a phishing email.

It is simply impossible for the banks to prevent phishing emails from being sent by fraudsters. The banks can only advise customers through the media and their websites not to click on any link in an email supposedly sent by the bank. The banks will never send emails to customer asking them to log onto their website or to confirm log in information.

Usage of public internet facilities is a further indicator that will be considered in respect of the compromise of information by means of key logging related fraud. The banks cannot prevent fraudsters from using key logging soft or hardware to trick unsuspecting customers. The banks can only warn their customers as advised earlier.

The terms and conditions of use of the bank's online banking facility

We also consider the terms and conditions of use of the bank's online banking facility as these normally contain clauses that excludes or limits the bank's liability where unauthorised access is gained to an account using the customer's legitimate access credentials.

Examples of such clauses would be:

- *You authorise us to carry out any and all instructions we receive through the access channel, including without limitation instructions that we debit your account, transfer money from your account, or provide information about your account, on condition that these instructions are authenticated by:*
  - *Your PIN and password, or that of your main users; and*
  - *Any other security measures/procedures that we may agree with you in writing from time to time.*
- *Unauthorised use of the PIN and password*
  If another person obtains your PIN, password or user number or those used by any of your main users, by whatever means, we will regard you as having authorised this person to use the access channel and to access your account on your behalf, as your agent with full authority to do so, unless you are able to prove that this person obtained the PIN, password or user number because we were negligent, or because of internal fraud perpetrated at the bank.
- *Limitation of liability for loss or damage*
  - *You acknowledge that your use of the access channel and your account is entirely at your own risk.*
  - *Accordingly, unless we acted with gross negligence or fraudulent intent or in breach of this agreement, we will not be liable for any costs, expenses, losses or damages of whatever kind which you or any of your main users may suffer or incur as a result of, arising from, or in connection with any unlawful or unauthorised or incorrect access to the access channel by any person other than yourself and your main users;*

The terms and conditions of use of the banks' online banking platforms therefore often state that, should a third party gain access to your PIN, password or user number, by whatever means, they will regard you as having authorised this person to use the access channel and to access your account on your behalf, as your agent with full authority to do so, unless you are able to prove that this person obtained the PIN, password or user number because of the bank's negligence, or because of internal fraud perpetrated at the bank.

Reporting times

We generally require banks to freeze fraudulent beneficiary accounts within a reasonable period of time after the unlawful access has been reported to them. If the fraudulent beneficiary accounts are opened at the same bank where the customer (the person who has been defrauded) has his account, this time period may be shorter than in the instance where money is transferred to accounts held at other banks. A further

consideration would be the number of fraudulent beneficiary accounts involved. The fewer fraudulent beneficiary accounts involved, the easier it should be to identify the accounts, the account holders and the banks these accounts are held with. In such an instance, it should take less time to freeze the accounts. The contrary, however, applies where more fraudulent beneficiary accounts are involved. Although the office considers certain time frames as guidance, each case will be evaluated on its merits.

Security features

Some banks have fraud detection systems, which enable them to rapidly detect fraud if the relevant triggers are activated. A fraud detection system is regarded as a bonus loss mitigating tool but is not, however, not mandatory. These systems, to be effective, work on highly confidential detection criteria and thus we do not investigate technical aspects of these systems.

Banks' internet banking systems differ and thus they offer different security measures. We do not compare banks' security offerings. We will, however, investigate whether a particular bank's security features were operational at the time of the fraud.

Banks also introduce new security features from time to time – these are not regarded as an admission of security deficiencies. Internet banking fraud is dynamic and its hallmarks change from time to time, as fraudsters constantly update or change their methods to find ways around the security measures. Although banks attempt to predict new trends, it would be impossible to make accurate forecasts and to align their security features accordingly. The banks close hundreds of false websites every day but the fraudsters will usually have numerous pre-constructed sites available to use as they are closed by the banks.

It should further be noted that customers of all banks with an internet banking offering have been targeted through this fraud phenomenon.

It is reasonably expected of the banks to warn their clients of these types of scams. Phishing fraud is not only widely publicised in the media but also on the banks' internet banking websites themselves. The banks posts regular warnings on their internet banking websites regarding this type of fraud and other associated topics. They also, from time to time, send notifications to their clients by means of SMS and email communications, not only in respect of this particular type of fraud but also stressing that they would never request a client to disclose or to confirm his/her confidential internet banking access details.

FICA compliance

The Financial Intelligence Centre Act 38 of 2001 (also referred to as "FICA") sets down certain requirements that the banks must meet when opening new accounts. Identity and residential address verifications in respect of all beneficiary accounts will be investigated. It should be borne in mind that third party account information is private and confidential and thus such information will not be made available to the customer lodging the dispute. We will, however, consider this confidential information when we make a finding in a specific case.

Fully verified accounts (using both identity and residential address) do not have any restrictions and the account holder can withdraw and transfer money as agreed with the bank.

Accounts opened in terms of the exemption 17 notice have certain restrictions. Amongst others, one cannot accept deposits of more than R25 000 over a period of a month and withdraw more than R5 000 per day from these accounts.

We will investigate whether these agreed or regulated limits had been complied with by assessing the transactional patterns on the respective fraudsters' accounts.

It is almost impossible to determine whether beneficiary accounts were opened using fraudulent information (fraudulently obtained ID and residential address documents) or whether the fraudster obtained a legitimate account holder's details by fraudulent means and was able to transact on the account. Investigations of this nature are more appropriate for the police.

The bank can only provide the account information to the police if it is served with an order of court.

Internet banking limits

Experience has shown that customers very often confuse their daily and/or monthly withdrawal limits with the daily and/or monthly limits being activated in respect of the internet banking facility.

If this aspect is disputed by a customer, we will investigate whether there is sufficient evidence of the customer's knowledge of the applicable limits.

Customers should familiarise themselves as to their applicable internet banking limits and the ways in which these limits could be changed.

SIM swapping

Cellular phone network providers are compelled to comply with certain legislative requirements before they activate a SIM card. The aim of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (also referred to as “RICA”) is to clamp down on the theft of mobile phones and mobile phone-related fraud.

A bank has no control over SIM swaps, as this is driven by the cellular phone network providers. Cellular phone network providers are required to take steps to ensure that SIM swaps are only granted with sufficient customer identification in accordance with section 40 of RICA.

Our office is regretfully not able to investigate the circumstances under which the SIM card replacement was approved. The request to do so does not involve the bank and our office therefore does not have the necessary jurisdiction.

The Ombudsman for Banking Services
Reviewed January 2018