



Consumer information note 8
Consumer information note 8

Internet Banking Fraud

Distribution: Media
Public

1 March 2011

Please note that the information provided 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 own 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 various internet banking scams and fraud. The purpose of this note is to describe the various 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:

Clause 2.9: The Fundamental Principles of our Relationship

*We, the members of the Banking Council undertake to:
...provide reliable banking and payment systems services and take reasonable care to make these services safe and secure...*

Clause 4.14: Internet and telephone banking

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

- ◆ *Review your bank statements and reconcile your accounts regularly.*
- ◆ *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.*
- ◆ *Check the site security certificate for the Internet banking site each time before you do your banking.*
- ◆ *Ensure that a temporary password is changed to a password of your choice known only to you.*
- ◆ *Should you be aware that your secret access code/ PIN/password or other unique means of personal identification has been observed by anyone, change it immediately.*
- ◆ *The security of your personal computer is your responsibility.*

- ◆ *Ensure that you read and are familiar with the Terms and Conditions of your bank's website and the product terms and conditions on the website.*
- ◆ *Enter numbers accurately when doing your banking and in particular with telephone banking.*
- ◆ *Ensure that you make payments to the correct account or beneficiary. We cannot reverse duplicate or erroneous payments you make to other accounts without the specific consent of the account holders.*
- ◆ *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.*
- ◆ *Ensure that there is adequate anti-virus and security software installed and enabled on the computer you use for Internet banking.*

Various types of internet banking fraud occur:

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 (also known as one time passwords (OTPs) or random verification numbers (RVNs)) in certain instances.

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

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. 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 they 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 (OTP/RVN) 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 such as creating new beneficiaries or to increase limits to name but a few.

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 in order to intercept the randomly generated once-off password (OTP/RVN).

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 (OTP/RVN).

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 (OTP/RVN) 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 e-mail 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 e-mail 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 it within the hardware unit. The attacker will retrieve the unit to access the keystrokes stored in it. Hardware key loggers can look similar to 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 has the ability to 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 have to unravel the keystrokes captured in order to use it 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 (account limits: available funds, overdraft limit or credit limit and monthly transactional 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 could the fraudster 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 are able to access the bank's internal computer systems so as 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 a number of aspects 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 are able to 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 exactly 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 the fraudsters will sometimes change the OTP/RVN delivery destination with the OTP/RVN compromised by the customer. This allows for all future generated OTPs/RVNs to be sent directly to the fraudster.

The banks will sometimes find evidence of the phishing e-mail that was received on the customer's computer. The information will show that the e-mail 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 e-mail.

It is simply impossible for the banks to prevent phishing e-mails 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 e-mail supposedly sent by the bank. The banks will never send e-mails 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 its customers as advised earlier.

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 being involved. The less fraudulent beneficiary accounts are 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 a shorter period of 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 own merits.

Security features

Some banks have fraud detection systems, which enable them to detect the fraud very soon if the relevant triggers are activated. A fraud detection system is regarded as a bonus loss mitigating tool, however, not mandatory. These systems, in order 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 constantly 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. The banks posts regular warnings on its internet banking websites regarding this type of fraud and other associated topics. It also, from time to time, sends notifications to its clients by means of SMS's and e-mail, not only in respect of this particular type of fraud but also advising 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 for the banks 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 information, albeit of a confidential nature, when we make a finding in a specific case.

Fully verified accounts (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 difficult if not 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 account details by fraudulent means and was able to transact on the account. Investigations of this nature are more appropriate for the police to investigate.

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 it could 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 regulate 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 regrettably is not in a position 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 jurisdiction to investigate such.

Should the complainant wish to take this issue further he can approach the Independent Communications Authority of South Africa (ICASA), which may be of assistance. They can be contacted as follows:

Mr Gumani Malebusha

ICASA

Tel no: (011) 321 8465 or (011) 566 3423

Fax no: (011) 448 1870

E-mail: gmalebusha@icasa.org.za and Consumer@icasa.org.za

Ombudsman for Banking Services