

## DEPOSIT AND REFUND SCAMS

Deposit and refund scams are on the increase and YOU may be at risk of becoming a victim. The deposit and refund scams work on the same premise: a fraudulent cheque is deposited and misrepresented either as cash or as an electronic funds transfer (EFT). The perpetrators will then create or amend a document to reflect the credited funds as being cleared. A cheque deposit slip will be amended to reflect as cash or a fraudulent internet payment confirmation will be generated.



### Features of a deposit scam

- Perpetrators approach a target with payment for goods or services.
- A deposit is made once the deal is concluded.
- The victim may or may not check their account to determine whether the funds have been credited. In some cases victims rely on the fraudulent document and assume its legitimacy in confirming the deposit, thereby releasing the goods or completing the service.
- The initial deposit, however, is in actual fact a cheque deposit masquerading as cleared funds. This amount is returned and the account is debited.

### Features of a refund scam

There are three refund scam scenarios:

#### 1 An unexpected credit reflects on your account.

- The perpetrators make contact, claiming that they had deposited funds into your account by mistake.
- They request a refund via EFT to a nominated account. In support of their claim you receive either an internet payment confirmation or a cash deposit slip.
- The claim of incorrect payment is sometimes supported by a fax, purporting to be from a well-known company or institution (Telkom, SARS, etc).
- You may be convinced that the funds are cleared and duly return the full amount to the nominated account.
- Days later the initial fraudulent cheque deposit is reversed and your account is debited. As you have 'refunded' the amount via EFT, the funds are immediately cleared and the fraudsters withdraw the amount and disappear.

#### 2 A new deal is concluded and a specific amount is expected in your account.

- You receive an internet payment confirmation or a cash deposit slip to confirm the deposit of cleared funds.
- However, the perpetrators make a deposit, that exceeds the expected amount (the new amount appears to be the result of human error – an extra zero or a double digit).
- Contact is made either from your side or from theirs. They claim ignorance and confirm the mistake on their part with an urgent request to have the funds returned.
- You may see the deposit reflecting – perhaps as 'movements due' or with a suitable narrative – and duly refund the difference on the basis of the amended deposit slip/internet payment confirmation.
- The cheque deposit is again unpaid a couple of days later and you carry the loss.

#### 3 The fraudsters intercept a company's debtor invoice.

- A cheque deposit is made in excess of what the debtor owes the targeted company.
- The fraudsters then contact the company (telephonically or sometimes by fax) and claim that they have made an electronic transfer in excess of the invoice 'received'.
- Similar to the scenarios described above, a document will be provided to mask the deposit as a cash deposit or an electronic transfer.



### Preventative measures

- Contact your branch or business manager to confirm the source of the deposit.
- Always insist on verification that the movements on your account represent a cash deposit or an internet transfer. Do not merely accept that it is in fact a deposit showing on the account.
- Delay the refund until you can obtain absolute confirmation of cleared funds in your account. Don't be bullied – it is common for the caller to be insistent, and sometimes even abusive, when he/she contacts you.
- Avoid using a non-personalised form of authentication (ATM/SST/Internet statement), as the perpetrators are adept at disguising the source of funds through fabricated narratives. Rather contact the bank, where the physical deposit can be viewed and it can be verified whether it was an EFT, cheque, cash or mixed deposit.
- Do not rely solely on the balance shown on the internet or at the ATM, as it may include a cheque deposit, which, because of your impeccable conduct of your account, is immediately available.
- Pay careful attention to the details reflected on the email or fax that you receive, as there are often telltale signs such as the following:
  - The letterhead reflects only a cellphone number as contact number and the only official numbers are the well-known client service numbers such as the 1023 facility.
  - The 'proof of transfer' document sent to you, often originates from one institution, yet the refund is to a totally different institution.
  - Obvious spelling and grammar mistakes.

If you suspect that you are a target of fraudulent activity, contact the South African Police Service (SAPS), as well as your branch or business manager, with as much detail as possible and, if the originals are unavailable, ask for clear copies of all the documentation involved. In conjunction with the legal authorities, Nedbank Group Forensic Services uses this information to track the syndicates and implement controls in an attempt to prevent these types of fraud from occurring again.

You can also visit the following sites on the internet for more comprehensive information on deposit scams:

- [http://www.obssa.co.za/news\\_041029\\_new\\_scam.htm](http://www.obssa.co.za/news_041029_new_scam.htm)
- <http://www.persfin.co.za/index.php?fSectionId=592&fArticleId=3399972>
- [http://www.saps.gov.za/org\\_profiles/core\\_function\\_components/commercial/deposit\\_scam.htm](http://www.saps.gov.za/org_profiles/core_function_components/commercial/deposit_scam.htm)
- [http://www.news24.com/Regional\\_Papers/Components/Category\\_Article\\_Text\\_Template/0,,1806-1810\\_1743832~E,00.html](http://www.news24.com/Regional_Papers/Components/Category_Article_Text_Template/0,,1806-1810_1743832~E,00.html)
- [http://www.sars.gov.za/media/media\\_releases/2006/Urgent%20scam%20warning%20-%2024%20August%202006.htm](http://www.sars.gov.za/media/media_releases/2006/Urgent%20scam%20warning%20-%2024%20August%202006.htm)
- <http://www.moneyweb.co.za/economy/tax/961087.htm>
- <http://www.carteblanche.co.za/Display/Display.asp?Id=2929>

### Contact numbers:

Nedbank	0860 555 111
Old Mutual Bank	0860 555 222
Pick 'n Pay Go Banking	0860 654 222
Client Retention Unit (complaints helpline)	0860 444 000
Business Banking (commercial)	0860 103 870
Small Business Services	0860 116 400



MAKE THINGS HAPPEN

NEDBANK  
CORPORATE

BUSINESS BANKING

A Member of the  OLD MUTUAL Group

## KEEPING YOUR CARD AND PIN SAFE

As the industry moves towards virtual banking, the products offered give you the ability to conduct your banking outside of a branch at all times. Over the years the card has evolved from an ATM withdrawal card to a full-service banking mechanism. The Nedbank cards provide you with access to ATMs, self-service terminals (CSSTs) and now merchant purchases as well.

Previously the card's impact on your account was governed by your daily withdrawal limit. However, with the card giving you access to transfers, purchases and your account profile, this product has become very attractive to fraudsters. Syndicates have developed various ways of gaining access to your accounts without having to visit a branch, thereby decreasing their risk of exposure. Ways of gaining access include:

### Card swapping

This occurs when a legitimate card is physically swapped for a fraudulent card. Either the person who swaps the card or his/her accomplices observe your personal identification number (PIN), which gives them access to your accounts. The PIN can be observed via camera or by shoulder-surfing (where someone stands out of sight and physically observes you as you enter your PIN).

### Card skimming

The legitimate card is swiped through a skimming device before being returned to you. The devices can be small enough to hold in the palm of a hand and record the account information with one swipe. This information is later encoded onto a blank card. Magnetic-strip cards and the recording devices are legally available to anyone who wishes to purchase them. The physical skimming of the card is either perpetrated in plain sight, where you believe it is being swiped through a legitimate point-of-sale (POS) device, or via sleight of hand, where the device is hidden from view. Again, your PIN is observed and noted and will later be used to access your account.

### Card theft

The theft of a card occurs in many different ways. The perpetrators tamper with ATMs so that the card appears to be swallowed, or lift the card while you are using it to pay for purchases.

These scams occur at ATMs, where one person or a group of people approach you while you are using the machine and states that it is out of order, or offer assistance. They are highly skilled and most of our clients do not even suspect that their card ever left their possession. This can also occur at a retail store, a restaurant or even a petrol station.

It is important that you select a PIN for your card at the time of issuing. The information is encrypted and staffmembers do not have access to the information. The only way the PIN can be recorded is through visually recording it. Regardless of when you use the card, it is important to shield the PIN entry with your other hand. Should you have any suspicions that your PIN may be compromised, immediately contact your branch and have the card blocked.

### Prevention guidelines

- Ensure that you sign all your cards as soon as you receive them.
- Protect your cards as if they were cash.
- Be alert to what is happening to your card when performing a transaction.
- Be aware of your surroundings and don't allow yourself to be crowded at an ATM. When waiting in line, stand well behind the person or persons using the ATM and ensure that the person queuing behind you keeps a reasonable distance from you.



- Stand close to the ATM and shield your movements with your hand and body when keying in your PIN.
- Only key in your PIN when prompted to do so by the terminal, not when requested to do so by a stranger.
- Never enter your PIN if the card appears to be stuck.
- Check that the card returned to you after every transaction is in fact yours.
- Refrain from spending excessive time at an ATM. Draw your money and leave – for example don't rummage in your bag/briefcase, or make notes in your diary.
- If your card is lost, stolen or retained in an ATM, cancel it immediately (tollfree numbers are displayed on the ATM).
- Be wary of 'helpful' strangers who offer you cellphone assistance to cancel your card. If you accept the help, check that the number dialled is the same as the tollfree number displayed on the ATM. Report all incidents of ATM crime to the bank and the police.
- Retain transaction slips and check them against your statement. Query unauthorised debits as soon as possible using the relevant contact numbers on your statement.
- Reduce your daily or monthly limit at your branch to match your average usage. Excessive limits will increase your exposure if your card is stolen or skimmed.
- Regularly check that you have all your cards with you.

## IDENTITY THEFT

Identity theft is the primary cause of all fraud-related cases. Perpetrators take advantage of legitimate and well-established clients by assuming their identity either to misappropriate their funds or to apply for credit using their credentials.

Identity theft takes many forms. Certain particulars may be used, such as a victim's postal or residential address, or his or her full identity may be assumed. Most victims only find out about the pilfering of their details when they try to apply for credit and discover that they have been listed at various credit bureaus for bad debt. Trying to prove that you have not applied for the credit is difficult and to have your record cleared even more so.

Most of the time, you are probably giving out your information without knowing it. Various scams are in place to obtain your information, such as fake competition forms and phishing websites. However, it is far easier to obtain the necessary information by going through your rubbish bin or your car when it is cleaned or by stealing a handbag. Many people don't think when they discard their mail that they are giving out ID numbers, addresses, contact numbers, account numbers and even bank statement details. In addition, your post may be intercepted, where identifiable mail is removed and perused for sensitive information.

### Follow these guidelines to help protect your identity:

- Store your personal and sensitive information in a secure place. Ensure that your filing cabinets are kept locked and your mail and documents are filed away. Refrain from leaving documents lying around, even in your home, where contractors, visitors and even family members may have access.
- Destroy your personal and financial information by shredding the paper or tearing up and disposing of the pieces in different places.
- Never write down passwords, personal identification numbers (PINs) and the like. Keep them in your head, or if you do require a reminder, rather note a clue.
- Pay attention to postal cycles and enquire if you don't get a bank/financial statement by the usual date. Review your financial statements regularly to detect any unknown movements on the accounts.
- Don't carry unnecessary information around with you, such as bank statements, payment receipts and certified copies of your identity document in your bag/wallet. These items can be easily stolen.



MAKE THINGS HAPPEN

NEDBANK  
CORPORATE

BUSINESS BANKING

A Member of the  OLD MUTUAL Group

- Never keep your identity document and driving licence together, if they are stolen, you may have a hard time proving who you are.
- Don't disclose personal information on the internet, unless on secure sites.
- Don't disclose personal information when asked to do so telephonically or via email.
- Never respond to SMSs asking you to send your details via SMS to qualify for anything.
- For PINs and/or passwords avoid obvious choices such as birthdates and first names.
- Never keep these details on your PC, as they can be recorded by software or viewed by hackers.
- Don't use internet cafés or unsecured terminals (hotels, conference centres, etc) to do your banking, as the data can be easily intercepted.

**If you are a victim of identity theft:**

- Notify your creditors in writing of the problem.
- Report the matter to the SAPS.
- Alert the South African Fraud Prevention Services (SAFPS) immediately on 0860 101 248 or at [www.safps.org.za](http://www.safps.org.za). They will list the identity theft on their database to prevent further credit from being granted in your name.
- Contact Experian/ITC/KreditInform to ensure that you have not been blacklisted due to non-payment etc.
- You may have to consider closing existing and opening new accounts.

