ombudsman for banking services
SOUTH AFRICA

Bulletin 12

Card Cloning

Background

The office receives a number of complaints relating to card cloning. This issue is of serious concern worldwide and often receives significant media attention. We have issued several recommendation reports on card cloning matters but it is appropriate that the office issues a bulletin in this regard advising banks and their customers of the approach we take on claims of this nature.

The cloning process

What is card cloning?

Card cloning or counterfeiting can be described as a process whereby a genuine bank card's magnetic-stripe is copied and then placed on a duplicate card. This cloned card can then be used to make purchases at point of sale devices and (where the customer's personal identification number [PIN] has also been obtained) to make withdrawals from Automated teller machines (ATM).

The process whereby the card's magnetic stripe is copied is generally known as skimming. The card is swiped through a skimming device similar to those found on point of sale devices. The information on the magnetic stripe is then recorded and is then placed on another card's magnetic stripe. Point of sale devices and ATMs are not able to discern the difference between a cloned card and the original as the information on the magnetic stripe is identical. If the thief has managed to obtain the customer's PIN he is then further able to make withdrawals from the account using an ATM.

Any type of bank card that has a magnetic stripe can be cloned. This includes credit cards, debit cards and normal ATM cards. Depending on the card holder's particular card processing systems however, the thief will not be able make any purchases or withdrawals unless he has also obtained the PIN. This would be the case with certain debit cards which also need the correct PIN to be entered on the point of sale device to process the transaction.

Point of compromise

There are numerous ways in which the thief can obtain the card to swipe it and copy the magnetic stripe information.

These methods can be summarised as follows:

- The placing of a card skimming device over an ATM's card reader. This device may be coupled with a small camera and recording device that records the PIN being entered on the ATM key pad.
- The swiping of the card by a teller or waiter through a skimming device while making payment at a store or business such as a restaurant, general goods store etc.
- The swiping of the card by a confidence trickster who convinces the card holder to hand over the card (and PIN) under the pretence of verifying the card, entering a competition or similar false claim.

Evidence of cloning

It can often be very difficult to determine whether a card was cloned. The customer will often approach the bank disputing that he made or authorised certain purchases or withdrawals on his account. The bank then must investigate the matter to determine the cause of the loss. As the ATM and point of sale systems cannot differentiate between a genuine and a cloned card, one should look at the surrounding circumstances of the claim. A conclusion then must be drawn as to what happened based on the probabilities.

The best evidence for cloning is where two separate transactions take place within a short time of each other at different locations far apart, making it impossible for the same card to have been used. We have dealt with matters where two separate transactions took place in Johannesburg and Cape Town within a few minutes of each other. This evidence will clearly suggest that the card had been cloned.

Cases where cloning may have occurred tend to display certain characteristics.

- The fraudulent transactions take place soon after an incident occurs where the card holder is approached by a stranger regarding his bank card.
- The card holder made a purchase at a store suspected to be involved in card cloning, just before the fraudulent purchases took place
- The maximum amount is withdrawn from the account until the account is depleted or the account is frozen (after the card is reported as stolen).
- The card holder is still in possession of his original card.
- The pattern of withdrawals and the amounts withdrawn are very different to the normal pattern on the account.
- The withdrawals or purchases take place at locations never used by the card holder before.

In many cases it can be difficult to distinguish a genuine card cloning incident from a so-called phantom withdrawal. Phantom withdrawals are cases where it is suspected that a person known or close to the card holder accessed the card and knowing the PIN, makes purchases or withdrawals using the card. The card is then returned to the card holder without him knowing that the card was removed or used. This can occur within family member groups, close friends or acquaintances. In these circumstances, the bank cannot be held liable as it is unable to prevent access to the card. Again, it is necessary to evaluate all the circumstances of the matter to determine the most probable cause of the loss.

The office and the banks must be on constant guard against fraudulent attempts by card holders to mimic a card cloning claim.

Chip and PIN

Due to the large losses sustained by the industry due to cloning, smart card technology is being introduced. Bank cards will now contain a chip which is generally very expensive to clone. A PIN is then also required to confirm any transaction. This technology has already been introduced in the United Kingdom to apparent success. According to recent reports there has already been a significant reduction in the losses suffered in the UK due to cloning. The technology has since also been introduced in South Africa which has led to a significant reduction in losses suffered due to cloning.

This technology is however not a cure-all. These new chip and PIN cards can still be cloned but it is not cost effective considering the expense required and the potential amount that can be stolen. Smart card technology is not used worldwide and smart cards must therefore still have a magnetic strip enabling it to be used in other countries. This magnetic strip can still be cloned and used for fraudulent purchases. Card cloning syndicates have now merely migrated to using the cloned cards in countries that do not have smart card technology. The criminal syndicates have further increased the use of other alternative methods of card fraud that do not require cloned cards, such as card-not-present fraud. Recent reports indicate that the overall losses due to card fraud have not dropped significantly.

Determining the relative parties' liability for the loss

Once it has been established that a card has been cloned, one faces the difficult task of deciding whether the bank or the customer is responsible for the losses incurred. There is no directly applicable case law or legislation regulating this issue and it must therefore be decided based on the relevant factors which are applicable. In deciding on this aspect,

the OBS looks at the contract between the bank and the card holder, the Code of Banking Practice and any applicable case law which can provide guidance. One then finally also investigates any possible negligence on the part of the card holder.

The contract between the bank and its customer

The terms and conditions applicable to a bank card are usually sent to the customer with the card. By accepting and using the card one is bound by these conditions. These conditions are generally very biased in favour of the bank. Each bank has its own conditions but they will generally state that the account holder is responsible for any transactions that take place on the account whether they are fraudulent or not. A strict application of the contract may therefore result in the card holder being held liable for all cloned card transactions.

The leading case that dealt with this issue is the matter of *Diners Club SA (Pty) Ltd v Singh and another 2004 (3) SA 630 (D)*. In this matter, the card holder disputed authorising certain transactions which occurred on his card in London. The case discussed numerous issues surrounding the encryption of the PIN and the possibility of a card being cloned. The clause of the contract stating that the card holder was liable for all PIN-based transactions was further challenged as being contra bones mores. The court ultimately held that the clause, although very one-sided and onerous, was not contra bones mores. The court went further however and made a negative finding on the actual credibility of the card holder regarding his testimony that he did not authorise the transactions. On the specific facts of the matter the court ultimately found that the card holder was liable for the amount owing on the account.

It can be argued that this case confirmed the absolute liability of the bank customer for any fraudulent transactions that take place using the customer's PIN. The reality however is that the banks would expose themselves to extreme reputational risk if it were to hold every bank customer liable in card cloning cases. It has further been suggested by academics that the conclusion reached by the court may have been different had the bank customer been an honest and truthful witness. This may have prompted the court to investigate the liability issue more closely.

One cannot ignore the terms and conditions as they form a binding contract between the parties. The OBS is however mandated to take all the relevant circumstances into account in issuing a recommendation, which may include issues of fairness and reasonableness.

The Code of Banking Practice

The office is mandated to use the law and the Code of Banking Practice (the code) when deciding on disputes.

The Code of Banking Practice contains the following provisions which are applicable:

3.2 Your responsibilities

The body of the Code that follows includes a number of responsibilities that your bank expects you to fulfill in your relationship with your bank. For ease of reference these responsibilities include the following:

- *Protecting your card and PIN is a crucial security measure for which you are responsible. You should never disclose your PIN, or other unique means of personal identification to anyone, including an employee of the bank.*
- *To enable us to take the necessary measures to prevent or limit fraud or theft on your account it is your responsibility to inform us as soon as possible when you discover any unauthorized activities on your account.*
- *When making use of our ATM services, you should take note of any cautionary notices that may be placed at ATMs for your protection, and exercise due caution accordingly.*
- *It is important to familiarize yourself with the circumstances under which you may be responsible for any losses suffered by you as a result of fraud, theft, or where you acted without reasonable care.*

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; similarly you are required to take due and proper care.

7.6 Cards and PINS

In order for you to access and transact on your accounts, we may issue you a card, PIN, password or other unique means of identification, or replace one that has already been issued, and may charge fees for this.

When we issue you with a card, we will ensure that the card and the PIN are issued separately and will take reasonable steps to satisfy ourselves that these have been received by you.

Where we issue you with a PIN we will take reasonable care to ensure that the PIN is issued in confidence. If you collect or receive your card and PIN personally, we will require proof of your identity.

Your PIN, password and other unique means of identification are strictly confidential. You

should never disclose your PIN, password, or other unique means of personal identification to anyone, and specifically not any employee of the bank.

We will tell you if you can select your own PIN, password or other unique means of personal identification and inform you of the procedures to change your PIN, password or other unique means of personal identification when the need arises. You may request your bank to issue additional cards, also called secondary cards. These cards will be issued to the secondary cardholders and they will be provided with their own PIN, password or other unique means of personal identification. You will however be responsible for all transactions relating to the secondary cards. You may request your bank at any time to cancel a secondary card, in which case you must ensure that the secondary card is destroyed or returned to the bank – if you do not do it, you may be liable for the use of the card.

7.7 Protecting your account

Please ensure that you keep us informed of any changes to your personal information, including any changes to your name, address, phone number or e-mail address.

Taking care of your chequebook, savings account book, cards, electronic purse, PINs, passwords and other unique means of personal identification is essential to help prevent fraud and protect your accounts.

Always ensure that you:

7.7.1 do not keep your cheque book or your PIN and cards together;

7.7.2 do not allow anyone else to use your card, PIN, password or other unique means of personal identification;

7.7.3 always take reasonable steps to keep your card, PIN, password and other unique means of personal identification secret, safe and secure at all times; never

disclose your PIN or password to anybody, including family, friends or any bank employee who offers to assist you;

7.7.4 never write down or record your PIN, password or other unique means of personal identification. If you must write it down, ensure that it is not accessible to others and that it is disguised. For example, never write down or record your PIN using the numbers in the correct order;

7.7.5 are alert to the risk of muggings, card swapping and other criminal activities when using ATMs or other electronic banking devices;

7.7.6 do not use PINs that are easy to guess, such as 1111 or 12345 or your date of birth, and use your card with care.

7.7.7 You may be able to subscribe to receive transaction notifications via sms that may be used to alert you of unauthorized activity on your account.

It is critical that you tell us as soon as possible if you suspect or discover that:

7.7.8 your cheque book, savings account book, cards and/or electronic purse have been lost or stolen;

7.7.9 someone else knows your PIN, password, information about your accounts or personal information or your other unique means of personal identification; or

7.7.10 there are transactions on your accounts, which you have not authorised;

7.7.11 take care when storing or getting rid of information about your accounts. People who commit fraud use many methods, such as retrieving statements from bins, to get this type of information.

In cases of theft or fraud, we may also need you to open a case with the police services and we will provide you with the necessary information to facilitate this with the police.

We will publish the contact details in statements, at ATM's or through other means of communication to you, which you should use to report lost or stolen cards or cheque books or to advise us if your PIN, password or unique means of personal identification has been compromised.

When you report that a cheque book, savings account book, card or electronic purse has been lost or stolen or that your PIN, password or other unique means of personal identification has been compromised, we will give you a code or reference number. Please keep this number for future reference, as this is your proof of having reported the loss or theft.

You should treat your electronic purse as cash in a wallet. You may lose any money left in the "e-cash" part of the electronic purse at the time it is lost or stolen, in just the same way as if you lost your wallet.

Please be aware that you may be vulnerable to crime when you use certain ATMs. You should adhere to any notices of caution at ATMs in order to protect yourself against crime. In particular, be wary of anybody who comes near you or attempts to distract you while you are using an ATM.

7.8 Responsibility for losses

After you have informed us that a cheque book, savings account book, card or electronic purse has been lost or stolen or that someone else knows your PIN, password or other unique means of personal identification, we will take immediate steps to prevent these from being used to access your account.

You will be liable for all losses, if you acted fraudulently. You may also be liable for losses, if you acted negligently or without reasonable care and this has caused or contributed to losses. This may apply if you fail to follow the safeguards set out in paragraph 7.7 above.

Furthermore, you may be liable for losses if you have not informed us as soon as reasonably practicable after you discover or believe that your secret codes or devices, if any, for accessing the e-banking services have been compromised, lost or stolen, or that unauthorized transactions have been conducted on your accounts.

Unless we can show that you have acted fraudulently, negligently or without reasonable care, we will refund you the amount of any transaction together with any interest and charges associated with the disputed transaction in the following circumstances and after consideration of all the facts:

7.8.1 where you have not received your card and it is misused by someone else;

7.8.2 for all transactions not authorised or effected by you after you have reported loss or theft of your card or chequebook or that your PIN may be compromised;

7.8.3 if additional money is transferred from your account to your electronic purse after you have informed us of its loss or theft and you have informed us that someone else knows your PIN, password or unique means of personal identification;

7.8.4 where system malfunctions have occurred in ATMs, or associated systems, which were not obvious or subject to a warning message or notice at the time of use (we will have to investigate each matter separately); or

7.8.5 where a credit card transaction is disputed, we accept the burden of proving fraud or negligence or that you have received your card. In such cases we expect you to co-operate with us and with the police in any investigation.

Please note, however, that we will not be liable for any losses caused by circumstances that are beyond our reasonable control, such as the following:

7.8.6 your inability to access internet banking, or any other application associated with or reliant on internet banking, at any time, or any failure or delay in providing a service via the internet;

7.8.7 a malfunction of any equipment (including telecommunications equipment) which supports our ATMs and internet, telephone or cell phone banking service;

7.8.8 your inability to access telephone or cell phone banking, or any other application associated or reliant on telephone or cell phone banking, at any time, or any failure or delay in providing a service via telephone or cell phone or

7.8.9 a disruption of services caused by political actions or natural disasters.

The bank has a responsibility in terms of the Code of Banking Practice to "*provide reliable banking and payment systems services and take reasonable care to make these services safe and secure*". Where a payments system is open to abuse the bank is expected to take reasonable measures to ensure that it is safe. This then means that the bank has the responsibility to ensure that ATMs and other means of transacting (such as cards) are reasonably protected from being tampered with by thieves.

The bank would thus be liable for any withdrawals done with a cloned card where the cloning was a result of tampering with a payments system such as ATMs and ATM cards that was not reasonably foreseeable or preventable by the card holder.

Case law

This approach would appear to be onerous on the bank but is based on the same approach taken by the courts in related instances. In the matter of *Kwamashu Bakery Ltd v Standard Bank of South Africa Ltd 1995 (1) SA 377 (D)* the Court held that:

"…it offended against fairness and reasonableness that a bank, which voluntarily decides to participate in a situation that has the inherent and well-recognised risk that the collection of a cheque might prove to have been for someone not entitled thereto, should be entitled to complain and state that it should not be held to a duty of care to deal carefully with that cheque because it would cost too much or disrupt its practice too much: the bank had been free not to accept such cheque. In any event, the evidence demonstrated that the banks inter se did not regard it as too onerous a duty for a collecting banker to ensure that it collected only for the named payee."

The Court further held that banks could recover the costs involved in ensuring that the depositor was the true owner from its customer by way of a service fee or the drawer could be levied with an additional fee for the use of a non-transferable cheque.

In the case of *Energy Measurements (Pty) Ltd v First National Bank [2000] 2 All SA 396 (W)*[1] the court specifically considered the steps a bank should take when opening an account for a new business customer. The court specifically found that banks in practice foresee the reasonable possibility that by opening accounts, such accounts may be used for fraudulent purposes that could cause patrimonial loss to the owners of stolen cheques. Reasonable steps, such as those of reasonable men carrying on the business of bankers, should be taken to protect themselves and others against fraud.

Although the cases dealt with cheques, the principle is very clearly applicable to card cloning. The banks provide a payment and transaction system in the form of ATM and credit cards to their clients knowing that it carries an inherent risk of being cloned. It is further aware that PIN numbers are fraudulently obtained by confidence tricksters which enable thieves to make withdrawals with these cards. The bank cannot merely close its eyes to the inherent risk associated with these cards and contractually hold the client liable. The bank has a duty of care to prevent this type of fraud despite the extra cost or effort in doing so.

International ombudsman approach

The Australian Ombudsman, in its policy and procedure document, refers to the Electronic Funds Transfer Code which states that: "*the fact that an account has been accessed with the correct PIN, whilst significant, will not in itself be conclusive evidence that the cardholder has contributed to the loss*". It goes on further to state that "*access with the correct access method will not in itself constitute proof on a balance of probability that the user contributed to the losses*". Where the Bank cannot produce evidence that the accountholder authorised the transaction, the Australians have found the accountholder is not liable for the amounts of the transactions and the interest and fees charged by the Bank in respect of the disputed transactions.

The United Kingdom Banking Ombudsman also supports the above approach. In issue 46 of the "Ombudsman News" a case study was used regarding cardholders' negligence for disputed withdrawals. The Ombudsman in this case stated that: "*if a firm believes that a cardholder is seeking to disown transactions that they did make or authorise, or that were made by someone who acquired the card with the cardholder's consent, it will not usually be enough to say simply that the cardholder was (or must have been) grossly negligent*." It went on further to state that: "*if a card issuer believes that the cardholder carried out the transactions, or authorised some to do so, then we would expect the firm to provide us with reasons for that belief, and any supporting evidence*".

[1] 1 Referred to and approved in *Columbus Joint Venture v Absa Bank Ltd [2002] 1 All SA 105 (A*)

Disclosing the PIN

Based on what we know from our investigations and what we have been shown, one cannot make withdrawals from an ATM without the card and the correct PIN. The PIN is further not stored on the card itself. In most instances where the thief uses the cloned card to make withdrawals he would therefore also need to know what the PIN is for the card. The thief can obtain the PIN as mentioned above by observing the complainant entering the PIN on an ATM or point of sale key pad or by recording it on camera. There have also been instances where the thief is able to convince the card holder that he is a representative from the bank and needs the PIN to verify that the card is legitimate.

The question that then arises is whether the complainant must be held liable for disclosing the PIN to the thief. Card holders are expected to take reasonable precautions to prevent their PIN being disclosed to others. Generally, this would require that the card holder does not voluntarily disclose their PIN to another person in circumstances where he reasonably should have been aware that it was unsafe to do so. In at least two of the instances mentioned above (camera device and point of sale transaction) it can safely be argued that the victim of cloning could not reasonably have been aware that their PIN is being disclosed to a thief or that the card is being skimmed. There is no reasonable basis for arguing that a customer can be expected to diligently search the ATM or teller area for hidden cameras, skimming devices etc. before making a withdrawal or tendering a card for payment.

It will therefore be important for the bank to determine how the card was cloned and the PIN observed as this may be the only way it can show that the card holder was negligent in disclosing their PIN. Only if the card holder was negligent can a conclusion can be drawn that the bank is possibly not liable for the fraudulent withdrawals.

One is often able to determine when the compromise of the card and PIN took place based on when the fraudulent transactions started. The thief will normally try to make the cloned card as quickly as possible and therefore the withdrawals will generally take place shortly after the card was cloned. We have received reports from the banks of instances where the cloned card was made and used within 45 minutes after the skimming took place.

The card holder is often reluctant to disclose that they were approached by strangers and that their PIN may have been observed. It is therefore necessary to evaluate all the surrounding circumstances to determine how the card may have been cloned. We must further be mindful of the possibility that card holders can attempt to defraud the bank by providing their card and PIN to others or by making the withdrawals themselves. It is further possible that the card holder innocently forgot about the withdrawals he made.

We must evaluate each case on its own merits to determine whether these are likely explanations for the losses.

Bank customer's duty to mitigate losses

Due to the high number of incidents of card cloning the banks have introduced various measures to try and limit the losses suffered. One of these measures is the use of a Short Message Service (SMS). Most of the major banks offer this service that provides for an SMS to be sent to the customer's cell phone every time a transaction takes place on the customer's account. This can potentially alert the customer to fraudulent transactions on his/her account and the bank can be informed immediately.

We fully support this service and actively encourage bank customers to make use of it. The banks however sometimes argue in cases before us that the use of this service by the customer limits or completely excuses the bank from any liability for any fraud that has taken place on the account.

When evaluating a case where the bank sent messages to the customer, alerting him to the fraudulent transactions that are taking place on his account, there are certain factors that we consider.

The SMS service offered by the banks is generally not a free service. At most banks, the service has to be paid for by the customer. Many customers are not able to afford the extra cost for the service. A customer can therefore not be held responsible or liable for fraudulent transactions on the basis that he/she did not have the service activated on the account.

Even if the service is activated on the account (at a cost or for free) this does not automatically place a general onus or responsibility on the customer to alert the bank to fraudulent transactions. The service is generally offered or granted to customers as an extra benefit. Generally, the customer is not warned that the use of this service will place a contractual duty or general obligation on the customer to alert the bank to fraudulent transactions and that any failure to react to the message may result in the customer being held liable. There is usually no specific agreement by the customer to such an obligation or increased risk.

Should the bank add such a contractual clause increasing the customer's liability and obligations we will evaluate whether the customer was reasonably made aware of these conditions and agreed to them.

The average bank customer is not constantly alert to the possibility of fraud taking place on his bank account. Bank customers are not reasonably expected to be extra vigilant 24 hours per day and to react at a moment's notice to any potential fraud taking place on their accounts.

It is therefore not reasonably expected of a customer to ensure that they have their cell phone with them when travelling internationally and to ensure that they have very expensive international cell phone roaming services activated.

It is not reasonably expected of customers to ensure that they react to an SMS that is sent to them in the middle of the night when they are asleep.

It is not reasonably expected of customers to ensure that they receive an ATM slip every time they do an ATM or internet transaction and to carefully scrutinise it to check that the balance available is the exact amount that they should have available.

The above examples demonstrate our approach to some of the bank's arguments regarding mitigation of losses which we have dealt with in this regard. They serve to illustrate our general views and approach and should not be considered exhaustive.

Having mentioned these aspects, we will however never disregard any reasonable expectations placed on the customer to mitigate his/her losses. There are numerous instances where we may well find that the customer was negligent in not responding to the messages or information received and reasonably should have alerted the bank. These are instances where, for example, the customer received numerous messages of fraudulent transactions during the day, read them but did not contact the bank at any stage. There are instances where the customer saw the balance in the account was reduced by a huge amount relative to the balance and reasonably should have alerted the bank to the problem immediately.

Each case will always be judged on its own merits.

Conclusion

The surrounding circumstances of each matter must be investigated and evaluated to determine whether a card was in fact cloned.

If the card is found to have been cloned, the relative liability of the parties involved must be established.

The bank cannot make a bare allegation that the customer must have been negligent in some way. The bank must produce substantial evidence or argument that the card holder was negligent and is therefore responsible for the losses incurred. It is impossible to specify what would constitute substantial evidence or argument as each case would be evaluated on its own merits. While we fully understand and appreciate the difficulties a bank will face in producing such evidence, this is the only viable approach that can be taken. The bank is undeniably in the best position to gather evidence in this regard or to take steps to limit its risk and exposure. Except in the most obvious and rare of cases it would be impossible for a bank customer to prove a negative assertion - that he was not negligent when his PIN and card was compromised and then cloned.

Any decision made will be based on a balance of probabilities.

The Ombudsman for Banking Services
Reviewed January 2018