



Bulletin No 13
Bulletin No 13

CARD CLONING

Distribution:

Members of Banking Association of South Africa
Representative Bodies
Other Financial Service Ombudsmen
Consumer NGOs
Government Consumer Bodies

28 January 2008

Background

The office receives a number of complaints relating to card cloning. This issue is of serious concern world wide and often receives significant media attention. We have issued a number of 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.

Recent reports by APACS (the United Kingdom payments association) show that losses due to cloning amounted to almost 100 million pounds in 2006. This equates to approximately 1.4 billion rand. Information as to the extent of the losses in South Africa is not readily available. It is however significant that the losses are generally reported as 'industry losses'. It is unknown what proportion of the losses is actually borne by the customer, not the bank. There is no available data on this proportion.

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 so as 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 allegation.

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 has to investigate the matter to determine the cause of the loss. As the ATM and point of sale systems cannot differentiate between a genuine or cloned card, one has to look at the surrounding circumstances of the claim. A conclusion then has to 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 one will have to evaluate all the circumstances of the matter to determine the most probable cause of the loss.

The office and the banks must further 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 it is busy introducing smart card technology. 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. South Africa is still in the process of finalising the introduction of the smart card to its bank customers.

This technology is however not a cure. These new cards (based on the technology used) can still be cloned but it is not cost effective considering the expense required and the possible amount that can be stolen. Smart card technology is not used world wide 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, has 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 making a decision 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 authorizing certain transactions which occurred with 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 bonos mores*. The court ultimately held that the clause, although very one-sided and onerous, was not *contra bonos 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 authorize 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:

THE FUNDAMENTAL PRINCIPLES OF OUR RELATIONSHIP

We, the members of the Banking Council undertake to:

- 2.1 act fairly and reasonably in all our dealings with you;*
- 2.9 provide reliable banking and payment systems services and take reasonable care to make these services safe and secure;*
- 4.8 Cards, PINS, passwords, and other unique means of personal identification*
- ◆ We may issue you a card, or replace one that has already been issued, and may charge fees for this.*
 - ◆ Your PIN (Personal Identification Number), password and other unique means of identification are strictly confidential. Where a bank supplies these, they will be issued only to you, separately from your card where applicable. 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. We will encourage you to avoid birth dates and simple sequences numbers such as 1111; 12345 and so on.*
 - ◆ We will inform you of the procedures to change your PIN, password or other unique means of personal identification when the need arises.*
 - ◆ We will publish the contact details you should use to report lost or stolen cards or chequebooks in statements, at ATM's or through other means of communication to you.*
- 4.9 Responsibility for losses*
- 4.9.1 After you inform us that a chequebook, 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.*
- 4.9.2 Subject to sections 4.9.3 and 4.9.4, we will refund you the amount of any transaction together with any interest and charges associated with the disputed transaction:*
- ◆ where you have not received your card and it is misused by someone else;*
 - ◆ for all transactions not authorised or effected by you after you have informed us (and we have given you a reference number) of the information listed in 4.9.1 (except “e-cash” transactions which we cannot audit).*
 - ◆ if additional money is transferred from your account to your electronic purse after you have informed us of its loss or theft (and we have given you a reference number) and you have*

- ◆ *informed us that someone else knows your PIN, password or unique means of personal identification; or*
 - ◆ *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.*
- 4.9.3 *If you act fraudulently you will be liable for all losses. If you act negligently or without reasonable care and this has caused or contributed to losses, you may be liable. This may also apply if you fail to follow the safeguards set out in sections 5.11, 5.13 and 5.14.*
- 4.9.4 *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.*

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 in order to protect themselves and others against fraud.

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

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 account holder authorised the transaction, the Australians have found the account holder 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”*.

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

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 absolutely 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.

Adv John Simpson
For: Ombudsman for Banking Services