ombudsman for banking services
SOUTH AFRICA

Bulletin 9

ATM Banking

The purpose of this information note is to provide background to the types of Automated Teller Machine (ATM) scams that occur, guidance as to how they should be investigated and to clarify how the Ombudsman for Banking Services (OBS) evaluates complaints of this nature.

The ATM complaints that our office receives generally relate to a certain category of incident. The instances mentioned below set out the most common types of complaints and how the incidents may have occurred.

ATM card reader jammed-card retained

The complainant proceeds to the ATM with the intention of making a withdrawal. Unknown to the complainant a thief has inserted a foreign object into the ATM card-reader: this causes the card to become stuck in the card-reader. After the complainant has inserted his card the ATM does not respond in any way, because it does not register that a card has been inserted. The screen does not change or request the person to enter his Personal Identification Number (PIN). The victim then enters his PIN in the hope that the ATM responds. He often also presses the cancel button to retrieve his card. The card is, however, not ejected. The complainant, thinking the ATM has legitimately retained his card, then leaves. The thief, who had been standing nearby, has seen the complainant enter his PIN and is now aware of what his PIN is. After the complainant leaves, the thief removes the object that he placed in the card reader and retrieves the card. He then rushes to the nearest ATM and draws as much money from the complainant's account as the system permits.

Card reader jammed-card swapped

Another variation on the abovementioned scam is the card-reader jam and swap. Here the thief jams the card reader with a foreign object. As soon as the victim unsuccessfully tries to insert his card into the ATM, the thief approaches offering to help. The thief then puts his hand over the victim's card as it is inserted into the card reader and by means of sleight-of-hand he then substitutes an old card he had in his hand with the victim's card. He then inserts this old card into the ATM and requests the victim to enter his PIN. The victim, thinking his card has been inserted, enters his PIN. The thief, now having seen the PIN and being in possession of the card, disappears to another ATM nearby to withdraw. In the meantime, the ATM indicates to the victim that the card is invalid and has been retained. Alternatively, the ATM does not recognise the card that has been inserted and does not respond at all. The victim then leaves, thinking he will contact the bank later to get his card back. When he does contact the bank, he is then informed that withdrawals have been made from his account. The thief might use accomplices to observe the PIN if the victim insists on the thief leaving the area while he enters his PIN.

It is also possible that the thief can approach the victim before the card has even been inserted making it unnecessary for the thief to tamper with the card reader in advance.

Thin plastic sleeve

This scam involves the thieves putting a thin, clear, rigid plastic 'sleeve' into the ATM card slot. When the victim inserts his card, the ATM cannot read the strip, so it repeatedly asks him to enter his PIN number. Meanwhile, someone behind him watches as he taps in his PIN.

Eventually the victim leaves, thinking the ATM has swallowed his card. The thieves then remove both the plastic sleeve and the card, and withdraw from the victim's account.

Assistance in phoning the bank to cancel the card

Many people are still being tricked by this old scam. It involves the card being swapped by various means as described above. The thief then offers to call the bank's lost card division on the victim's behalf using his cell phone. The victim, after speaking to the supposed lost card division, is brought under the impression that his card has been cancelled. In fact, he has spoken to a member of the criminal syndicate and the card is not reported as stolen. The method may either be used to obtain the victim's PIN (the syndicate member asks the victim for his PIN under the guise of it being necessary to cancel the card) or it can be used to delay the reporting of the card.

There are various other ways in which the ATM scams can be perpetrated. They all however involve a similar theme: observing the complainant's PIN and obtaining the card in such a way that the complainant does not realise what has happened. The crime can also be committed by a team of thieves simply distracting the complainant as the money is ejected or a deposit is made and then stealing the cash or deposit envelope.

The Code of Banking Practice

All our decisions on ATM complaints are generally based on the law, the Code of Banking Practice (the Code) and the principle of fairness. The bank often refers us to the terms and conditions document sent to card holders. This document essentially holds the complainant liable for any transaction on the account, whether fraudulent or not. The terms and conditions must however be evaluated in conjunction with the Code. To a large extent all the relevant terms and conditions are in any event reflected in the Code.

The following clauses of the Code are specifically applicable to any ATM-related complaint:

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.

Information needed when dealing with ATM complaints

The main problem associated with ATM complaints is to determine what in fact happened at the scene. The complainant will often only provide us with a very short overview of what happened. He may only state that his card was retained at the ATM when he wanted to make a withdrawal and that he later discovered that withdrawals had been made from his account. It is expected that banks will commence the investigation of any complaint relating to ATMs as soon as it is reported, in terms of the principles detailed below, irrespective of whether the complaint is finally reported to the OBS or not.

It is essential that the bank obtains a clear and detailed, step-by-step version of what happened at the ATM from the complainant at the outset. In addition to this, relevant background information should be obtained from the appropriate sources.

The lists of questions below serve as a guideline for gathering the information from the respective sources (some of the questions will only be applicable to certain banks depending on their individual systems and processes).

Information to be obtained from bank sources

1. Were the recommended site standards complied with at the ATM where the incident occurred? Furnish an ATM incident monitoring report / risk profile for the ATM concerned, to indicate whether the ATM was tampered with or not? (if applicable and relevant)
2. Did the ATM have a video camera on site? If so, preserve the video footage for review.
3. Can it be confirmed that the ATM had no malfunction or problem at the time of the incident?

4. Provide an accurate record of the transactions concerned, with times and places etc., together with the relevant Audit trail + Tally roll.
5. When was the call to cancel the card received?
6. Provide an account statement showing which transactions are in dispute.
7. Did the client make any statement to the bank regarding the incident? If so, provide us with a copy thereof.
8. Can the bank provide any evidence as to the identity of the person that withdrew the money from the ATM.?
9. What are the complainant's daily withdrawal limits for his ATM card?
10. Were the limits increased or decreased by the card holder? If so when?
11. Does the complainant have any secondary cards linked to his account? When was the card and PIN issued? Were new cards and/or PINs requested and when? When was the card cancelled?

Information to be obtained from the Complainant

1. Kindly advise what transpired at the ATM step by step.
    - What did the ATM prompt you to do and at what stage?
    - Did you receive the money requested from the ATM?
    - Was anyone near you or in your vicinity at the ATM?
2. Indicate on your statement which transactions you are disputing.
3. Where did you keep your card and how did you keep a record of your PIN?
4. Were you alone at the ATM? Was any other person within the vicinity of the ATM? Were there any people near you at the ATM? Was anyone present when you tried to withdraw money? Did you speak to anyone while at the ATM?
5. Did you ask anyone for assistance? Did anyone assist you? Did they possibly see your PIN?
6. When you inserted your card did the screen change in any way?
7. Did you enter your PIN at any stage while you were at the ATM? If so, at what stage?
8. Did the screen prompt you to enter your PIN? If not, why did you enter your PIN?
9. Did you phone the bank's lost card reporting number after the card was retained?
10. On precisely what date and at precisely what time did you report your retained card to the bank?
11. Why did you not report the card as lost when it was not ejected by the ATM?
12. Kindly advise whether any third party may have had access to your card and PIN?
13. Have you had any secondary cards linked to your account?

Once we have all the relevant information referred to above we may be able to make a finding on what happened at the ATM. This involves an objective evaluation of the facts available and drawing a conclusion on the most likely sequence of events, based on the established facts. It is often very difficult to make a finding which is consistent with the version of both parties. If we are unable to reconcile the complainant's version with known or likely scenarios (as referred to above), we would generally be unable to make a finding on what happened and would thus be unable to make any finding as to liability.

Once we have made a finding on what must have happened, we would be able to carry out an evaluation of the merits of the matter and make a finding as to liability.

Evaluating an ATM crime related complaint

The evaluation of an ATM-related complaint involves a weighing up of the various factors that contributed to the loss being incurred by the complainant. These factors can include (but are not limited to) the finding we make on the following factors:

- How the thief obtained the PIN.
- Whether the ATM was tampered with in some way.
- Whether the bank took reasonable precautions to prevent ATM crime occurring at that ATM.
- Whether the ATM in question had a history of ATM-related crime.
- Whether the ATM had cameras or any other form of additional security installed to prevent ATM crime.
- Whether the thieves used physical force against the complainant to obtain the card.
- Whether the complainant reported the loss of the card to the bank within a reasonable time.

Approach to ATM crime-related complaints

The bank has a duty, in terms of the Code, to provide reliable banking and payment systems services and to take reasonable care to make these services safe and secure. The bank therefore has a duty to take reasonable precautions to prevent ATMs from being tampered with or being used as a means of stealing money from card holders.

The card holder also has a duty to take reasonable precautions at an ATM to prevent his card or PIN from being stolen or observed.

In card swapping scenarios the victim often allows a person to assist them when they are struggling to insert their ATM card into the ATM card reader. This allows the thief, using sleight-of-hand techniques, to swap the victim's card for another and creates the

impression that the victim's card has been inserted into the ATM. The complainant is therefore tricked into believing that the card has not been stolen. The victim is expected to report the loss of the card to the bank. Any unreasonable delay in doing so is can be regarded as negligent. The question however arises as to whether the victim had sufficient reason to believe that his card had been lost or stolen. When the card is retained by the ATM under circumstances as described above, the victim is often under the impression that his card has legitimately been retained by the ATM and is not lost or stolen. He therefore does not report the card as lost or stolen to the bank.

An assessment will be carried out as to whether the card-holder was adequately warned in this regard or whether he reasonably should have known of the dangers, based on the circumstances of the incident. Each case would have to be assessed on its merits to determine whether the victim's belief in this regard was reasonable or not. All relevant factors and evidence are considered when evaluating the complaint.

The approach taken above is in accordance with international standards but allows for the uniqueness of the South African situation. Countries such as North America, United Kingdom and Australia have codes of conduct limiting the loss to a negligible amount. These countries do not however appear to experience the same type of ATM crime that is perpetrated in South Africa and therefore a more general policy, which looks at all the surrounding circumstances, is more appropriate here.

In deciding on a fair outcome, we are generally guided by the two key elements of the crime – the ATM tampering and the observing of the PIN. Both factors, irrespective of the way in which they were done, contribute to the eventual loss suffered. In appropriate circumstances, we will recommend that the bank bear a certain percentage (i.e.50%) of the total loss suffered by the complainant. Each case will however be assessed on its merits to determine an appropriate award (if any).

Debiting of account to which stolen funds have been transferred

A bank may generally not unilaterally debit an account, to which a suspected fraudulent transfer has been made. However, it is commonly found that accounts are opened with the single intention of receiving fraudulent transfers. Where a transfer has been made resulting from an ATM related incident as described above, it would be reasonably expected of the bank to 'freeze' the account to which the transfer has been made, pending an investigation. The bank could give notice to the account holder that his account may have been used for the purposes of an illegal transfer and that the funds will be returned to the victim. We have had instances where the bank was able to recover some of the funds transferred under these circumstances without objection. Each case would be evaluated on its merits.

Time of call to stop the card

A common dispute which arises in many complaints is the time of the call to cancel the card. As clients become more aware of the need to report the card quickly, the time taken to get through to an operator and provide the correct information becomes critical. The thieves also act immediately once they have obtained the card and the PIN. We have dealt with numerous cases where the call to cancel the card was made before the time of the fraudulent withdrawal but the card was only cancelled seconds or minutes afterwards. The bank then denies responsibility for the withdrawal. In these circumstances, it can be said that the complainant has done all he can to report the card in time, he cannot be held responsible for the time it takes to cancel the card on the system. While the logistics and necessity of verifying the card holder's account details before the card can be cancelled is noted, there is nothing more the complainant can do to ensure the process is immediate.

In the interests of fairness and the spirit of the Code the time at which the card was reported as lost or stolen will be taken as the time the call is made to the call centre, not when the call is answered or the card is stopped on the system. Therefore, should the call to stop the card have been made before the withdrawals had taken place, the bank will be expected to reimburse the complainant for those fraudulent withdrawals. Should the call have been made after the fraudulent withdrawals, all the factors mentioned in this bulletin would then still be applied and evaluated to determine an appropriate award (if any).

In this regard, we endorse the actions of at least one bank that reimburses clients for losses in certain circumstances even if the call was made after the fraudulent withdrawals had taken place. The bank in question evaluates ATM claims based on all the principles set out in this bulletin.

Phantom withdrawals

So-called 'phantom withdrawal' complaints involve the account holder reporting unauthorised ATM withdrawals from his account. The account holder will deny ever losing possession of his ATM card or that anyone has had access to his PIN. The complainant will then hold the bank responsible for the withdrawals.

To investigate these types of complaints we would need the following information from the bank and complainant:

- A bank statement from the complainant in which he clearly identifies the withdrawals he disputes and when he noticed the withdrawals the first time.

- Confirmation from the bank that only one card was allocated and issued to the complainant.
- The tally rolls for each disputed transaction which will indicate whether the card and PIN were used to make the withdrawal.
- The location of every ATM from which a disputed withdrawal was made and whether the complainant had made withdrawals from those same ATMs previously.
- Confirmation whether the complainant's card could have been duplicated (cloned).
- Information as to where the card is ordinarily kept and whether anyone else has access to it.
- Information as to whether the PIN was recorded or divulged in any way

Considering all the relevant information we may then make a finding on a balance of probabilities as to whether the bank was in any way responsible for the fraudulent withdrawals.

Disputed withdrawals

The complainant will allege that the ATM did not eject the cash after he had requested a withdrawal or that the actual cash dispensed was less than what he requested.

We will need the following information from the bank:

- The tally roll for the transaction concerned
- The electronic journal showing the number of notes and denominations dispensed.
- Proof that the physical cash in the ATM was reconciled and balanced. We would need the actual document signed by the ATM custodian showing the actual amounts which were counted and compared.

Once we have this information we may make a finding as to whether the money was dispensed or not.

Disputed deposits

The complainant will state that he deposited a certain amount of money at an ATM. When receiving his account statement, it then reflects a deposit of a lesser amount or that the deposit envelope was empty.

To investigate complaints of this nature we would need the following from the bank:

- The ATM audit trail listing the deposits made for the relevant ATM

- Statements from the ATM custodian staff who removed the envelope
- The documents signed by the staff noting the disputed deposit
- Extracts from the relevant manual noting the procedure followed in removing ATM deposit envelopes
- Any video footage of the removal and opening of the envelope
- Where cash is deposited directly into the cash acceptor, without an envelope, the balancing report and device journal indicating cash inserted and cash found in the cash presenter.

Once we have this evidence we may be able to make a finding on liability.

Conclusion

ATMs are used by most bank customers for cash withdrawals and general banking transactions. While we acknowledge that losses due to ATM crime forms a small percentage of the total number of transactions performed daily, it is very important that bank clients are satisfied that ATM banking is safe. If ATM banking is not perceived to be safe it could have dire consequences for the banks.

The various steps in preventing losses to customers due to ATM crime include the following:

- Informing customers of ATM related crime and methods to prevent it
- The banks taking reasonable physical precautions in making ATMs safe and secure from crime on an ongoing basis
- The banks settling reasonable claims for losses incurred due to ATM crime

Any complaint received regarding ATM crime will be evaluated on its own merits and in accordance with this information note.

The Ombudsman for Banking Service
Reviewed January 2018