SIBONGILE TAURAI ZIMBEVA
versus
KINGDOM BANK LIMITED

HIGH COURT OF ZIMBABWE
TSANGA & CHITAKUNYE JJ
HARARE, 10 September & 1 October 2014

Civil Appeal

R. Zimudzi, for the Appellant
M. Chitewe, for the Respondent

TSANGA J: This is an appeal against the decision of magistrate court in which the appellant Sibongile Zimbeva sought to recover an amount of $7548-91 from the respondent Kingdom Bank Ltd emanating from unauthorised withdrawals from her account by someone using her automated teller machine (ATM) card and PIN without her authority. In addition, the appellant also sought interest at the rate of 18% per annum being the lending rate of the respondent. She also claimed costs of suit on an attorney client scale.

The magistrate court having dismissed her claim she hereby appeals against the conclusion that the bank was not negligent in any way and that it bore no responsibility for her loss.

The facts

The undisputed facts are these. The appellant maintained an account with the respondent, Kingdom Bank Ltd, hereinafter called the Bank. She had been a customer for over eight years. She also had an ATM card as part of that account and could obtain cash from the respondent's various machines including those from related banks that were on the ZIMSWITCH system. On the afternoon of Sunday 20 January 2013, she attempted without success to withdraw some money from one of the Bank's ATMs at Karigamombe Building in Harare's city centre. Having failed to find cash thereat, she proceeded to yet another of the Banks ATMs located in First Street. There again she did not find any cash. Still resolute in getting some cash, she proceeded to Ecobank, a different bank altogether, to use her card on the ZIMSWITCH system which allows customers from participating banks to draw cash from

related ATMs. However, as emerged in evidence, Ecobank was not on the ZIMSWITCH system and therefore her assumption was erroneous in this regard. What is of significance with regards to her attempt at getting cash from Ecobank's ATM is that while in the process of trying her card for the second time in their machine, she was disrupted by a man who was behind her who urged her to hurry. She stepped aside and allowed him to proceed, all the while with her card in her hands according to her testimony. She said neither of them got any cash and each proceeded to their respective cars.

In a fourth bid to get the much needed cash, she headed to yet another of the respondent Bank's ATMs, this time at Fife Avenue shopping centre. Thereat her efforts came to a halt when her card was captured by the ATM with the message that the card was "stolen". She reported immediately to the guard who was policing the ATM who noted the card's capture in his daily occurrence book, together with her identity number, her cell phone number, and the time the report was made.

The following day, after putting in some work at her place of employment, the appellant utilised her lunch hour to retrieve her card from the Bank and to get the much needed cash. After being told that her card would be back at her branch within three or four days, she sought to make a personal withdrawal. It was in attempting to process this transaction in person that she was told that she had insufficient funds in her account. Her testimony was that her account balance on 20 January 2013 stood at $9863-28. When she attempted to transact on 21 January 2013 at lunch time the balance now stood at $2314-00. Since she had tried to withdraw $2500-00 it was in light of this that she was told her funds were insufficient. She immediately highlighted that any transactions on her account were unauthorised and the Bank instantly blocked her card against further transactions. She had however, already been prejudiced of an amount of $7 548-91. Notably the transactions totalling this amount were carried out in different stores and supermarkets using appellant's card on 21 January 2013 which was after her report of the card's capture on 20 January 2013 to the security guard.

As plaintiff in court below, the appellant approached the magistrate court claiming the sum of $ 7548-91 with interest after the respondent (as defendant) refused to assume responsibility. Materially in evidence in the court below the card which the Bank said it retrieved at its Fife Avenue ATM on 21 January 2013, did not belong to the appellant but to one Mr G Zimanga. The Bank averred that the appellant's card was not in their custody on

20 and 21 January 2013 as her card was eventually retrieved from High Glen on 22 January 2013 following the report of unauthorised transactions and its disablement made on 21 January 2013. However, the appellant disputed that it was not her card that was captured insisting that her card could have been removed from the machine by the Bank's employee. In her view this was likely so given the fact that the unauthorised transactions took place from the morning of 21 January 2013 which was when the Bank itself would have retrieved captured cards from the previous day, which was a Sunday.

In the court below, the appellant admitted to disclosing her PIN to her sister in trust as a backup measure for periods when she had travelled out of the country leaving her two children in her custody. Her sister's evidence was that although she knew the PIN, there was no occasion that had ever arisen requiring its use. In refusing the claim, the court noted the disclosure of the PIN as a material breach of the contract between the bank and its customer. It also placed emphasis on evidence provided by the Bank's witness, its Loss Control and Investigations Manager, that from the facts, the reasonable inference was that the appellant was a victim of a scam and that her card had been most likely exchanged at the Ecobank ATM. This was in the Bank's view more likely so since the card captured at the Fife Avenue ATM gave her the message that she was in possession of a stolen card followed by the fact that the card retrieved as having been captured at the time recorded, did not belong to her but to a Mr G Zimanga.

Her claim having been dismissed the appeal is to this court on the following grounds.

1. That the appellant suffered loss in the sum of $7 548-91 from the unauthorised withdrawals made between 20 and 21 January 2013 due to the respondent's negligence and or breach of duty of care in protecting depositor's funds.
2. The court *a quo* erred at law by failing to consider that the respondent was not entitled to debit the appellant's account without her specific mandate.
3. The court *a quo* erred by failing to consider the fact that the appellant carried out he responsibility and obligation to protect her own interest against fraud and exploitation by third parties.
4. That the court erred by failing to consider that the loss suffered by the appellant was a result of negligence by the respondent after the respondent had been duly notified by the appellant that her card was captured by the respondent's automated teller machine.

There is no specific legislation in Zimbabwe at present that addresses liability of banks for unauthorised ATM and POS withdrawals without a customer's consent. Any liability for refunding unauthorised withdrawals stems from the contractual relationship between a bank and its customer to protect the customer's funds. To protect customers from would be abusers banks generally place reliance on risk minimisation. Key measures include requiring customers to have a secret PIN to their card. Where a customer discloses such PIN to a third party, then from the bank's point of view, a breach of secrecy will have occurred with the result that it cannot be held responsible for the consequences stemming therefrom. Besides ensuring that withdrawals are effected through secret pins to the card, safety measures by some banks also include security measures at the ATMs, for example through camera surveillance, and in some cases through the provision of security guards who play some monitoring role. In addition, 24 hour reporting measures which permit a customer to contact the bank in the event that a card is lost or stolen are another protective measure. In *casu*, the first two of the Bank's ATMs where the appellant tried to withdraw did not have CCTV surveillance although the third had in addition to having a security guard. The PIN was also a security measure of its card issuance as was the 24 hour reporting service.

The contractual duty on the part of the customer is to guard the PIN and card "with their life" separately for the most part, save when transacting. The assumption by the bank is that only the customer has control of both these items. The duty to report is also on the customer particularly since unauthorised withdrawals come to the attention of the bank via the customer.

In arguing the Bank's duty of care the appellant places reliance on the following cases: *West Minister bank LTD* v *Hilton* (1926) 43 TLR 124 @126; *Lipkin Gorman* v *Karpnale Ltd* 1989 1 WLR 1340*; Barclays Bank Ltd* v *Quistclose Investments (Ltd)* 1970 AC 567. That as a general principle the Bank owes a duty of care to its customers is itself not in dispute. What is disputed is whether these withdrawals were indeed unauthorised so as to fall into the realm of negligence on the part of the bank which authorised them. At the gist of the appellant's argument is that processing withdrawals based amounting to $ 7 548-91 **after** the capture of the card had been reported a day earlier, was negligence in the extreme on the part of the Bank. The appellant's argument is that all transactions on this card should have been halted from the time that the Bank was notified through the security guard, that the card was

no longer in the customer's possession. According to her, it was the Bank's duty thereafter to ensure that no transactions were conducted against her account at least other than by herself in person, until such time that the card had been safely returned in her hands.

Adequacy of measures taken to protect the account

The appellant's argument that her report to the security guard at the Bank was a full line of defence in protecting her card calls for analysis of the contractual relationship between the parties involved. The record from the court below suggests that the exact parameters of the role of the security guard in relation to the bank were not fully canvassed. However, from the record, the reason given by the Bank's Loss Control Investigations Manager for having a security guard at the ATM is so that they can ensure no one interferes with clients when they do their transactions. The purpose of the entry by the guard was according to this witness a confirmation that a client made a report to the security guard of an anomaly.

Of significance is that generally, security firms work to fulfil the objectives given to them by their client. In other words, their contractual relationship is with their hirer. The reasons for which they are sought differ according to context. With respect to those hired to police specific locales, these generally include watch duties, in particular surveillance as well as protection of life and property. In our context, at ATMs they are often observed to manage people by requiring that they maintain a distance from a transacting party as also emerged from parts of the record.

In essence, their services are generally aimed at risk management as opposed to acting as a direct interface between a bank and its client. As evidenced by what is in the record, in carrying out a surveillance role, they record any reported anomalies and complaints that may have taken place on the given day including staff who may have come to the bank and their stated purpose. As such, theirs appears to be a routinized collection of information which is availed to the bank so that it at least has a starting point should this information be required. It cannot be said that reporting to the security guard absolves a customer from taking any other action on their card as the contractual relationship between a customer and a bank is a completely different one. The contract between the bank and a security firm remains at all times separate from the contract that the bank has with its client. The presence of a security guard at the premises should not be mistaken to establish a new type of contract between the

customer and the bank whereby the security guard is seen as acting as an agent of the bank. That is not the case.

In assessing whether a report was fully made to protect her account, this was a bank with a 24 hour reporting service where customers can reach the Bank regarding their account in the case of complaints or anomalies. There were essentially two abnormal though interlinked events which needed to be brought to the immediate attention of the appellant's Bank once her card had been captured. The first was its attempted use at a bank which was not at that time on the ZIMSWITCH system. The second was the clearly out of place message that her card which she transacted with, had given the message that it was "stolen". The record shows that the appellant herself, in her subsequent letter of complaint to the Bank, conceded that this message induced a sense of "shock" yet she still did not contact the bank on the given day nor did she attempt to go there first thing in the morning as a matter of urgency as would have been expected under the circumstances.

The Bank's argument that additional measures are to be followed by way of telephoning the Bank directly on its 24 hour service seems to be the crucial protective measure that ought to have been taken. The evidence of the Bank's witness was that it has messages at all of its ATMs advising clients to contact the call centre which is open 24 hours whenever a client's card is captured. He explained that a stolen card is then disabled in the system. In *casu*, the appellant did not report her card as stolen. She went to collect her card on 21 January 2013 and it was only in attempting to withdraw cash following disclosure to her that her card would take a few days to return to her branch, that anomalies emerged with her account balance. It was then that it was immediately disabled.

The appellant did not challenge the Bank's witness in the court below on the adequacy of visibility of this message which the Bank said is there at all of its ATMs. It is therefore assumed that the signage is satisfactorily visible. Given the appellant's own concession in the court below that the message that had come on screen that the card had been stolen, it would reasonably have been expected under such circumstances that any person acting sensibly and protectively, would have taken additional steps to appraise the bank more fully of the abnormal message that came with the card's capture.

Without providing particulars to the Bank, it seems there was no reason for the Bank to suspect that the appellant's card was at risk. Only if a report had been made to the Card Centre can it be said that the bank would indeed have been negligent if after receiving a

direct notification it had not stopped transactions on her account. Merely reporting to the guard was not enough as the correlation between a report to a security guard and an automatic freezing of the card's transactions on the bank's system is simply not there. In *casu*, the guard merely recorded daily occurrences. If the appellant had indeed called the 24 hour service and spoken to an employee with detailed explanation of what had occurred, the Bank would most certainly have been negligent if it had gone ahead to authorise withdrawals against the customer's account. The Bank cannot be held responsible for unauthorised withdrawals when the appellant took no action on 20 January 2013 to appraise them more fully of her card's capture.

Breach of care in protecting depositors funds

The appellant's argument was also that the Bank was negligent in that it had stopped sending message alerts to its customers notifying them of any withdrawals also calls for analysis. The issue here is whether it can be said that failure to do so is sufficient to apportion the entire blame for the unauthorised transactions at the Bank's door. The Bank's explanation for not sending transaction alerts was that the system was being revamped and that the appellant was told she would have to register. If the customer was told that she needed to re-register then she should have done so. Clearly, if she had done so she would have been alerted to the first withdrawal, and the amount taken from her account would have been minimised. But what would have stopped these transactions altogether from taking place would have been a detailed report of the anomalies of the day that may have indicated that the card was at risk. As analysed above, any reports involving a customer's card are dealt with through a 24 hour service. It is the report received from the customer that alerts the bank if a customer's card is at risk. A card that is reported as showing a message that it is "stolen" would needless to say put any bank on the highest alert. It was the appellant's duty to appraise the bank in some detail of the events that had transpired.

The appellant also argued lack of authorisation on the basis that the withdrawals were not made by herself and whoever was making the withdrawals did not have her permission. She challenged the Bank's version that she was likely dispossessed of her card at the Ecobank ATM as she had her card with her at all times. The appellant relies on authorities involving cheque fraud to illustrate that banks have been found liable where such cheques have been processed without the customer's authority. The case of *Sino Zimbabwe (Pvt) Ltd*

v *Zimbabwe Banking Corporation Pvt Ltd* 2006 (2) 320 was cited in support of this contention. The appellant argued that the same reasoning must apply with equal force to ATM instructions. It can however be argued that forging a cheque is comparatively easier to do without authority since what one is essentially working with is a forged signature which many are able to do. The Bank's unwavering standpoint through their witnesses and counsel, was that to effect a transaction, the PIN and the card are needed for both ATM and POS withdrawals. It remains their argument that the Bank cannot be held liable where a customer has, through her own acts, compromised both the card and its PIN. In support of this argument the Bank cites the views of *Havenga et al* in their book: ***General Principles of Commercial Law***[1] where they state at p 416 as follows regarding the use of ATM cards and their PIN numbers:

> "If an unauthorised person gains access to a customer's ATM card and PIN, the possibility of an unauthorised withdrawal arises. The machine cannot determine whether the person who inserts the card and keys in the correct number is in fact an authorised person. The question is whether the customer may be debited with the amount of such an unauthorised withdrawal".

In answering this all important question the authors go on to state as follows:

> "The issue will usually not arise because most financial institutions offering ATM facilities conclude an express contract with their customers in this regard. The agreement provides that the customer's account may be debited with all withdrawals made by means of the particular card and accompanying secret number. Only if the bank is notified of a possible unauthorised withdrawal before it takes place will the customer not have to accept the debit."

They then state as follows with reference to situations where there may not be an express term:

> "There seems little doubt that the correct PIN entered by the customer is the customer's mandate for these purposes. However, it seems that in the absence of an express term there might quite possibly be a tacit term in the banker – customer contract that the customer would carry the risk of an unauthorised withdrawal. Surrounding circumstances which exist on conclusion of the contract play an important role when the court has to determine the intention of the parties. A customer who obtains an ATM card realises that the whole system functions by means of a card coupled with a secret PIN number. The person also realises that the identity of the person who inserts and keys the number cannot be checked. Against this background it seems reasonable to

[1] Peter Havenga et al *general Principles of Commercial law (Claremont: Juta 7th Edition, 7th Impression 2013) at p 416*

> assume that the customer consents to accept a debit for any withdrawal made by means of a card and number. It stands to reason that the customer will run the risk only until he or she informs the bank of the loss and possible unauthorised use of the card."

Applying these principles to the facts of the present case, there was in essence no effective reporting that would have stopped the transaction on the card. Indeed, once the bank was advised by the appellant on 21 January 2013 that there were unauthorised transactions, it immediately blocked the card and there were none thereafter.

Significantly, given that any withdrawals are both card and PIN based, the appellant's concession in the court below that she had disclosed her PIN to a third party further weakens her case in terms of the contractual requirements with the bank that the PIN remains secret. From the evidence in the court record, the bulk of the unauthorised payments from the appellant's account were done using the "electronic fund transfer at point of sale. (EFTPOS). As *Havenga et al* explain at p 418 of their book, a PIN is also used for these transactions. However, they do highlight that there are EFTPOS systems which use hand written signatures where after the customer's card is swiped, duplicate transaction slips are issued which must be signed by the customer. In such cases it is the signatures of the customer that identifies the user and gives authorisation to the bank to pay. A copy of the transaction slip is kept by the merchant and handed to the bank should a dispute arise. The bank will generally not pay if the merchant has not complied with verification of the customer's signature. The other copy remains with the client.

In *casu,* the Bank in its evidence insisted that the PIN and card was the method used to access the account. In other words they disputed that a card alone would have sufficed to use the card without a PIN. But clearly much depends on the type of machine used at the transaction. Nonetheless *Havenga et al* explain as follows with regard to EFTPOS transactions[2]:

> "The most important standard term as far as the customer is concerned is that defining the circumstances under which the bank is entitled to debit its customer's account. The general rule is that the customer is (at least initially) liable for all uses made of the card or PIN whether authorised by him or her or not. In some cases liability for unauthorised transactions is limited in terms of the contract, for example on informing the bank of the loss or card or PIN. A second term that is standard to all card

[2] Supra at p 419

> conditions is the obligation of the customer to keep the PIN secret. A third important term is that an EFTPOS transaction is irrevocable….."

In *casu,* the appellant's card and PIN were utilised thereby meeting the first standard condition regarding honouring payments using the card and PIN. The second condition that the PIN be kept secret was, as stated, violated by the appellant's disclosure to her sister. The third requirement that once made the payments could not be revoked explain why the Bank cannot reverse such payments if there is no evidence of being incorrectly carried out.

It also clearly does not help the appellant that she tried to use her ATM card at an ATM which was not supported by her Bank's system. Her narration of events of what took place in the form of her encounter with the man who disrupted her transaction lends credence to the Bank's assertion that it was possibly at Ecobank that her card was swopped. Whilst indeed the evidence on record was not conclusive that the card disappeared at Ecobank since the Bank's efforts to obtain CCTV footage from Ecobank had been unsuccessful, however, on a balance of probabilities, the events of the day lend support to the claim that the card and the PIN could have been tempered with at the Ecobank ATM. The fact that the card found in the respondent's ATM machine was not hers further lends credence to this theory of dispossession at the said bank's ATM. The appellant challenged the fact that the card was said to belong to Mr G Zimanga because it was retrieved out of the machine on 21 January 2013 and not 20 January 2013 and therefore could not have been the same card. The explanation by the bank that the card having been captured on a Sunday when banks were closed, it was only removed on the morning of the following day appears to have been a credible explanation. Even if the appellant's argument is taken of the possibility that the card was taken by a bank employee then the issue still arises of how they obtained the PIN. Granted the PIN could have been guessed but there is no evidence that suggests that this is what happened. Also it does not explain why as the appellant conceded, her card gave the message that it was "stolen". The failure to identify the fraudster captured on CCTV footage at two supermarkets using the card is of course lamentable as it would have gone a long way in clarifying the circumstances of the fraud.

In essence, looking at the various arguments put forward by the appellant regarding the Banks negligence and her own efforts to protect her account, as against the Bank's

arguments as to why it should not be held liable, the conclusion is that the appellant failed to take active steps to prevent the unauthorised use of her account.

In the circumstances the appeal lacks merit and is accordingly dismissed with costs.

Chitakunye J agrees:……

Hove & Associates, Appellant's Legal Practitioners
Chitewe Law Practice, Respondent's Legal practitioners