IN THE HIGH COURT OF UGANDA SITTING AT KAMPALA

COMMERCIAL DIVISION

Reportable
Civil Appeal No. 0028 OF 2023

In the matter between

STANBIC BANK UGANDA LIMITED **APPELLANT**

And

MOSES RUKIDI GABIGOGO **RESPONDENT**

Heard: 13 July, 2023
Delivered: 12 January, 2024

Banking — *Contractual liability of a banker for acts of nonfeasance — To determine negligence, the Court applies a flexible balancing test which weighs the burdens of imposing a duty on the bank plus the social utility of the ATM against the gravity of the ATM crime and the likelihood of its occurrence. – As a result, banks will only be liable for a breach of the imposed duty which occurs when the burden and utility weigh less than the gravity and likelihood of the harm.*

ATM Fraud and Digital banking. — The bank must produce substantial evidence or argument that the card holder was negligent and is therefore responsible for the losses incurred. —The customer will be liable for the loss occurring due to unauthorised transactions where the loss is due to negligence by a customer. — Where a security breach occurs at the ATM, the onus lies on the customer to prove negligence by showing that the bank in question could have done more to safeguard the integrity of customer's personal information from unauthorised access.

JUDGMENT

STEPHEN MUBIRU, J.

Introduction:

[1] For about ten years the respondent had operated a current account with the appellant bank, in respect of which he registered for internet banking by virtue of which he would use is registered mobile phone number to undertake transactions on his bank account. He was also issued with an Automatic Teller Machine (ATM) card, by virtue of which he was in position to deposit onto and withdraw cash from his bank account at various locations of the appellant's ATMs.

[2] The respondent's case in the Court below was that on or about 19th March, 2021 at around 10.30 am he accessed the appellant's ATM at its "Metro Branch," located on the NSSF Building along Kampala Road, intending to deposit a sum of shs. 2,500,000/= using one of the ATMs. He inserted his ATM card into the machine and keyed in the "deposit" option. He changed ahis mind, pressed the "cancel" button and tapped the "balance inquiry" option. The mini-statement printout indicated he had a credit balance of shs. 4,114,065/= on his account. He withdrew the card and inserted it afresh. This time round when he entered his PIN, the display screen showed "no deposit" which he understood to mean that he could not deposit cash using the machine. He pressed the "cancel" button once again but the ATM card did not come out immediately.

[3] As the respondent waited for the machine to eject the ATM card, out of the blue a hand of a stranger reached out across the respondent's shoulder from behind him, and simultaneously pressed the yellow and red buttons causing the card to eject immediately. The stranger then handed the ATYM card to the respondent, muttering words to the effect that the card had delayed to eject. The stranger immediately walked away as the respondent moved to the next machine to attempt the transaction once again. He inserted the card into that machine but on typing

his PIN, the machine returned a message on the user interface screen which read "capture" and printed out a receipt to that effect. The respondent was left with no option but to enter the banking hall and deposited the cash across the counter with one of the bank tellers. He requested one of the bank staff to retrieve the card from the machine but by the time he concluded the transaction the card had not been retried. He was advised to leave behind his contact details, which he did.

[4] Later that day at around 4.30 pm after receiving a call from the bank staff he had left with the card retrieval request in the morning asking him what his branch was, he shortly thereafter received a series of sms alerts on his mobile phone indicating that there had been various transactions on his account that left a credit balance of only shs. 1,650/= yet he expected it to be shs. 6,602,415/= He called back the bank staff, inquiring what had happened to the funds on his account. The bank staff asked him whether he had ben assisted by anyone while at the ATM. The following day the respondent returned to the appellant's "Metro Branch," where the security officers played back to him the cctv footage showing what happened the previous day while he was at the ATM. He saw that two men stood nearby and one was in close proximity to his left side, while he was transacting at the machine. The one to his left was so close that he must have observed him as he typed his PIN onto the keypad of the machine and possibly memorised it. It is the second one that came from behind him who offered the unsolicited assistance and caused the ATM card to be ejected. It ids that man who in the process had exchanged the respondent's card for a dummy, which he handed over to the respondent and took the respondent's genuine card with him.

[5] On 22nd March, 2021 the respondent then wrote two letters to the appellant's management regarding that incident. He later filled in the standard card holder complain form but never received any response to any of those complaints. He then sued the appellant contending that the loss of his funds was occasioned by the appellant's failure to deploy a security guard at the ATM and to monitor the

cctv. It is that failure that enabled strangers to accost him and defraud him later by carrying out unauthorised transactions on his account.

[6] In its defence, the appellant contended that upon the respondent reporting that his ATM card had been captured, it was successfully retrieved on the same day and the respondent was notified accordingly. However, although the "capture" notification receipt corresponded to the retrieved ATM card, it was discovered that the card did not belong to the respondent. Suspecting fraud, the appellant had proceeded to block the respondent's account immediately on the same day, 19th March, 2021. By that time the fraudster had already used the card to withdraw shs. 5,710,000/= from the respondent's account. The appellant contended therefore that the loss was occasioned by the respondent's negligence and that the appellant was not responsible for the actions of the security guards at the premises.

The judgment of the Court below;

[7] In her judgment delivered on 9th March, 2023 the learned trial Magistrate Grade One held that as a banker, the appellant owed the respondent a duty of care to protect money deposited with it by the respondent, as well as to secure the respondent's personal information furnished for purposes of his banking transactions. The respondent as customer expected to be afforded a safe environment while transacting at the ATM and that fraudsters would not have access to his PIN by getting close to him. It is common knowledge that using trickery, without the victim getting any much the wiser, fraudsters may gain access to a customer's PIN without any negligence or abetment on the part of the customer. The appellant has published on its official website, information providing tips to customers on how to prevent such fraud; including being alert and not permitting any distraction while at the ATM, choosing a familiar conveniently located ATM that is well lit, visible and safe, cancelling transactions immediately

where the machine is faulty and trying another, and to beware of strangers offering help as they could be engaged in a scheme intended to distract the user.

[8] These notifications showed that the appellant was aware of the risk such as befell the respondent. The bank only provided a caution but did not furnish detail on how such scams are perpetrated. This did not create sufficient awareness that ATMs may be compromised. Unfortunately, the cctv footage was never tendered in evidence. The parties nevertheless gave an oral account of what the recording showed. The appellant did not show how exactly the respondent was negligent. The respondent testified that he was shocked to see the hand of a stranger reach out across his shoulder. The respondent had not noticed the presence of that person behind him and his intervention was very swift before the respondent could realise what was going on. He did not engage with the stranger willingly. He did not willingly expose himself to the risk of fraud.

[9] A customer cannot maintain a proper look out for strangers around him, while at the same time transacting with the ATM. It is the duty of the bank to place security guards at the booths to prevent strangers from getting close to the person transacting. Such a guard would ensure that there is only one customer inside the booth at a time and prevent others from entering until the one inside is done. It was the respondent's testimony that this is the established practice. There was no security guard on the fateful day at that booth and that is why this happened. The appellant placed an unreasonable duty on the respondent to protect himself. The fraud could have been prevented had there been a security guard at the time.

[10] The Court found the appellant to have been negligent and to have breached its banker-customer relationship. As a result of that negligence and breach, the respondent lost a sum of shs. 6,602,415/= There is no evidence to corroborate the appellant's assertion that it blocked the card on 19th March, 2021 since the withdrawals continued until 24th March, 2021. That sum was awarded as special damages with inters at the rate of 24% per annum from the date of filing the suit

until payment in full, For the appellant's failure to take steps to protect the respondent from a type of fraud it was aware of, it was directed to compensate the respondent in the sum of shs. 5,000,000/= as general damages and additional sum of shs. 4,000,000/= as exemplary damages with interest on the two awards at the rate of 15% per annum from the date of judgment until payment in full, as well as the cost of the suit.

The grounds of appeal.

[11] Being dissatisfied with the decision, the appellant appealed to this Court on the following grounds, namely;

1. The learned Magistrate Grade One erred in law and fact in holding that the appellant was negligent and acted in breach of its banker-customer relationship with the respondent.
2. The learned Magistrate Grade One erred in law and fact in holding that the respondent suffered loss due to the appellant's negligence.
3. The learned Magistrate Grade One erred in law and fact in holding that the respondent's loss was not caused by any negligence on his part.
4. The learned Magistrate Grade One erred in law and fact in holding that the respondent suffered loss due to the appellant's negligent actions.
5. The learned Magistrate Grade One erred in law and fact in ordering the appellant to compensate the respondent with the lost amount of shs. 6,602,415/= which was not proved.
6. The learned Magistrate Grade One erred in law and fact in awarding the respondent general damages in the sum of shs. 5,000,000/=
7. The learned Magistrate Grade One erred in law and fact in awarding the respondent exemplary damages in the sum of shs. 4,000,000/=

Submissions of Counsel for the appellant;

[12] Counsel for appellant, argued that the terms and conditions of the ATM use at page 116 and 117 of the record show that the customer has the duty to safeguard the PIN. The respondent did not report the incident to the bank. At age 153 of the record, he admitted not alerting the security. Page 57 and 58 the police officer who testified stated the respondent did not protest and also had an interaction with the intruder. He instead immediately went into the bank and reported that his card had been retained and made a cash deposit of shs. 2,500,000/= There was no evidence of this type of fraud being rampant, on record, but the magistrate found it at the bank website at age 144. There was a warning of fraud of that nature. It was not a sudden approach by a stranger. The bank was not negligent. There were two machines at the same location; it is not possible to limit access to one person at a time. Page 62 line 14 at page 114 of the record the with statement para 9 the fraudster used interswitch and used ABSA and DFCU ATMs. The transactions were on the same day but they were posted later after reconciliation. It is when he was called that his card had been retrieved that it was blocked.

Submissions of Counsel for the respondent;

[13] Counsel for respondent, argued that the bank has to secure the ATM. The respondent came to the facility alone, operated the machine alone only that he took time to make a deposit which failed on the first attempt and on proceeding to the second machine a hand passed over his shoulder. The role of a security guard is to detect and act. In this case there was no security at the ATM. They play the role of bank security and should be available full time. They provide security, regulate access and at the same time monitor behaviour. D.W.1 at page 61 testified and confirmed that there should be security at the ATM but could not recall whether there was security on the day. *Ocaya Richard Sracen Ltd v. Saracen U Ltd and another, HC CS 23 of 2011* is a case in point. Had there been security this type of fraud would have been prevented. Page 60 of the record of appeal. P.W.1

testified that the machine took time to eject the card and the security guard was supposed regulate space between customers. Grace Patrick Tumwine Mukuubwa Cases in African Banking Law and Practice, states that the relationship between the bank and the respondent is contractual. The bank blocked the card but surprisingly the transactions went on. The incident was on 19th March, 2021 but the bank statement P. Exhibit "I" at page 94 the transactions went through on 20th up to 24th March, 2021. It is on the same day that the respondent reported the withdrawals. D.W.1 testified that the blocking was immediate. The withdrawal limit was shs. 5,000,000/= a day but from the transactions they exceeded the limit. In *Col. DS Sacha v. Punjab and Jund bank, RPN 1046 of 2003* ensuring safety of the money to be deposited and withdrawn inside the bank is the duty of the bank.

The decision;

[14] The appeal raises issues of contractual liability for a banker's acts of nonfeasance, i.e. the failure to take steps to protect another from harm, as distinguished from misfeasance, or active misconduct causing positive injury or loss to others. It is the respondent's case that the bank failed in its duty to protect him from the type of ATM fraud that led to the loss of his funds, while the appellant denies such liability and instead attributes the loss to the respondent's negligence. The facts that the relationship underlying the use of ATM cards is usually governed by extensive and detailed written agreements between the parties, as well as the fact that the amount involved in the average ATM card transactions is usually relatively small, few disputes regarding ATM card transactions ever reach the courts. Therefore, once it is established that a fraud was committed at an ATM involving use of an ATM Card, the Court faces the difficult task of deciding whether the bank or the customer is responsible for the loss incurred. There is hardly any authoritative directly applicable domestic case law or legislation regulating this issue and it must therefore be decided based on the relevant factors, on a case by case basis.

[15] Generally, in order to hold the appellant liable, the trial Court had to determine first whether the appellant's acts or omissions were the sole, direct, and proximate cause of the respondent's loss. On the other hand, to succeed in its defence, the appellant had to show that the sole, proximate cause of the loss complained of was the sudden intentional criminal act of an unidentified stranger, which could not have been prevented or deterred by the exercise of reasonable care by the Bank, but could have been prevented by the reasonable care of the respondent. It is necessary to evaluate all the circumstances of the matter to determine the most probable cause of the loss.

[16] It is the duty of this Court, as the first appellate court. to re-hear the case by subjecting the evidence presented to the trial court to a fresh and exhaustive scrutiny and re-appraisal before coming to its own conclusion (see *Father Nanensio Begumisa and three Others v. Eric Tiberaga SCCA 17of 2000; [2004] KALR 236*). In a case of conflicting evidence this court has to make due allowance for the fact that it neither saw nor heard the witnesses, it must weigh the conflicting evidence and draw its own inference and conclusions (see *Lovinsa Nankya v. Nsibambi [1980] HCB 81*). It may interfere with a finding of fact if the trial court is shown to have overlooked any material feature in the evidence of a witness, or if the balance of probabilities as to the credibility of the witness is inclined against the opinion of the trial court. In particular, this court is not bound necessarily to follow the trial magistrate's findings of fact if it appears either that she clearly failed on some point to take account of particular circumstances or probabilities materially to estimate the evidence or if the impression based on demeanour of a witness is inconsistent with the evidence in the case generally.

i. <u>Preliminaries.</u>

[17] Digital banking is the integration of digital technologies into the business model and overall organisation, including the provision of banking products and services through digital means and with a focus on customer experience. It expands beyond

banks and financial institutions: non-bank institutions (e.g. payment providers, credit card issuers, e-commerce and other digital corporations) are now part of the ecosystem. It presents a delicate balance regarding the interface of usability and security; a trade-off between technical security levels to protect customers from cybercrime losses on the one hand, and on the other the ease of use related to the willingness and capability of users to accept and adopt security measures, in the context of usable security of systems requiring multiple level tracking and multiple levels of authentication, without hindering efficiency.

[18] Cards issued by banks to enable electronic transactions usually comprise of three components, namely; the plastic card, the chip which is an embedded microprocessor and the magnetic strip. The card has embedded in it the customer account number, usually a multiple digit number serving as a unique identifier for each customer, and the customer's PIN, usually comprising four digits designed to be known only by the customer or persons to whom he or she discloses it. The sole purpose of the chip is to interact with terminals to enable cash withdrawals at automatic teller machines (ATMs) and to enable payments and transactions on the account. Transactions are initiated with the ATM card and are essentially authorised with an input of a PIN. The information in the magnetic stripe is used to identify the cardholder via the PIN. The PIN and the usage of the card constitutes the cardholder's electronic signature that authenticates the transaction. What follows is a series of prompts and inputs from the cardholder, where after a receipt of the cash marking the completion of the transaction, the card is returned. A debit entry is then entered on the relevant account.

[19] ATM cards issued by banks may be used by the cardholder to effect cash withdrawals at any ATM) of the issuing bank, and those by other banks which are linked to tan inter-bank network, to which the issuer of the card belongs, which allows for cross-bank ATM withdrawals (such as "Interswitch"). The standard terms of use normally stipulate that when the correct PIN is entered it is considered to be the customer's mandate and effect will be given to that instruction. The standard

agreement between the bank and the cardholder usually contains provisions in respect of losses which may be incurred as a result of the unauthorised use of the credit card. Banks usually contract out of the risk associated with electronic payments, specifically the liability for unauthorised electronic funds transfers. This culminates in bank's customers bearing the bulk of that risk as a result of the bank-customer contract. Apparently, there is currently no specific or dedicated legislation in Uganda covering electronic banking services. A number of aspects surrounding the use of electronic banking products are not necessarily covered by the provisions of *The Electronic Transactions Act, No. 8 of 201*1 or *The Electronic Signatures Act, No. 7 of 2011.*

[20] Whether victims of electronic banking frauds should be left to bear the loss themselves or whether losses should be redistributed by requiring banks which have made or received the payments on behalf of customers to reimburse victims of such crimes is a question of social policy for regulators, government and ultimately for Parliament to consider (see *Philipp v. Barclays Bank UK plc [2023] UKSC 25*). Legislators and regulators have the institutional competence to take an overall view of a perceived social problem and to consider the appropriate policy response as a whole and from a variety of angles after wide consultations, bringing together a variety of perspectives from persons with experience and expertise in relevant fields of knowledge, taking into account the relative costs and benefits of different possible measures, and thereby design a comprehensive regime containing qualifications, exceptions and safeguards. On the other hand, Courts are bound to apply the laws made by Parliament and to respect precedents created by past judicial decisions, in that process adapting and developing the common law to keep it up to date, but are required to proceed by reasoning from established principles and are under a duty to promote consistency and predictability in the law.

[21] Banking legislation in some other parts of the world has prescribed an explicit liability regime to address unauthorised debits to the accounts of ATM card users

due to negligence on the part of the card user or his or her bank or financial institution. In the United States, for example, *The Electronic Funds Transfer Act* provides for the protection of consumer rights in electronic banking and funds transfer systems. In particular, it establishes explicit provisions for consumer liability in the event of an unauthorised electronic fund transfer to the effect that the customer is liable "only if the card or other means of access utilised for such transfer was an accepted card or other means of access and if the issuer of such card, code, or other means of access has provided a means whereby the user of such card, code, or other means of access can be identified as the person authorised to use it, such as by signature, photograph, or fingerprint or by electronic or mechanical confirmation." Where the customer is liable for unauthorised transfer, such liability will not exceed 50 US dollars, or the amount of money obtained in the unauthorised transfer prior to notifying the financial institution that an unauthorised electronic fund transfer has been or may be made on the consumer's account.

[22] Because payment practices are changing faster than the laws and regulations that govern them, the assignation of liability when fraud occurs is quite complicated in Uganda's current legal landscape. Until the electronic-payment systems and electronic money products offered by banks are regulated by their own dedicated legislative measures, the relationship between the providers of electronic payment facilities (i.e. banks), on the one hand, and the users of such facilities (i.e. the customers of banks), on the other hand, will be regulated by those few provisions of the available statutes that apply or have a bearing to electronic financial services, read with the common law principles bearing on the law of contract. Given that the relationship between a bank and its client is generally in the nature of a contractor mandate, it may be surmised that the rights and obligations flowing from the contract of mandate will apply to the relationship between a bank that provides electronic banking services and its client who makes use of such services.

[23] The bank-customer contract is one of mandate. Under that contract, a bank is required to effect a customer's orders timeously once the instruction is given in accordance with the terms agreed between the parties. Where an ATM transaction is initiated using the card issued by the bank and the correct PIN entered, it would constitute an electronic signature signifying a payment order. The bank has a duty to carry out its customer's authorised payment instructions (where the customer's account is in credit). While the bank has a duty to exercise reasonable skill and care when effecting its mandate (see *Selangor United Rubber Estates Ltd v. Cradock (No 3) [1968] 1 WLR 1555; Westminster Bank Ltd v. Hilton (1926) 43 TLR 124; Barclays Bank plc v. Quincecare Limited [1992] 4 All ER 363; Royal Products Ltd v. Midland Bank Ltd [1981] 2 Lloyd's Rep 194 and Westminster Bank Ltd v. Hilton (1926) 43 TLR 124)*, the customer in turn has to effect the payment order with reasonable care so as to limit the chances of fraud and deception (see *Young v. Grote, 1827, 4 Bing. 253 and London Joint Stock Bank Ltd v. Macmillan [1918] AC 777)*. If owing to neglect of this duty, forgery takes place, the customer is liable for the loss. Otherwise, banks generally have the duty to compensate customers for fraud on their accounts provided the customers have not been grossly negligent, which is a degree of negligence where whatever duty of care may be involved has not been met by a significant margin; a very significant degree of carelessness.

[24] Cybercrime that targets electronic banking and payment services generally reduces consumer trust in electronic transactions and also impedes the adoption and penetration of electronic banking and payment services as well as e-commerce yet on the other hand imposing heavy, burdensome, or intrusive duties on banks stifles the growth of that industry, There is therefore a delicate balance to be struck between on the one hand imposing too burdensome an obligation on bankers thus hampering the effective transacting of banking business unnecessarily, and on the other hand guarding against the facilitation of fraud. Courts are generally reluctant to impose liability where existing banking statutes do not. To determine negligence, the Court applies a flexible balancing test which

weighs the burdens of imposing a duty on the bank plus the social utility of the ATM against the gravity of the ATM crime and the likelihood of its occurrence. As a result, banks will only be liable for a breach of the imposed duty which occurs when the burden and utility weigh less than the gravity and likelihood of the harm.

[25] Courts have established a five-factor policy test to apply when considering whether a particular set of facts warrants imposing a duty where such a duty was not previously recognised. These factors are: (1) the relationship between the parties; (2) the social utility of the actor's conduct; (3) the nature of the risk imposed and foreseeability of the harm incurred; (4) the consequences of imposing a duty upon the actor; and (5) the overall public interest in the proposed solution. No single factor, however, is dispositive. The courts must assign appropriate weight to each policy factor, depending on the particularised nature of the asserted duty at hand and context.

[26] Banks are not generally liable to make refunds, even where the customer has been tricked into paying the wrong recipient. On the contrary, a bank's principal duty is to obey its customer's mandate and, indeed, it may be liable to a customer if it fails to comply with a payment instruction. However, a bank may be liable in contract and/or negligence if it fails to take reasonable skill and care when executing a customer's order. The test is that a bank must refrain from executing an order (or cancel it where possible) where it is "put on inquiry" in the sense that it has reasonable grounds for believing that the order is an attempt to misappropriate the funds of the customer.

[27] The liability of the bank is commonly referred to as "negligence," without due thought as to whether the remedy lies in contract or in tort. Being a contact of banking, the mutual rights and duties of the two parties are regulated entirely by the contract, including in particular the duty of the bank to take reasonable skill and care when executing a customer's order. Common law has reiterated that a duty of care exists on both banks and their customers not to facilitate fraud. Where the

breach of duty alleged arises out of a liability independently of the personal obligation undertaken by contract, it is tort, and it may be tort even though there may happen to be a contract between the parties, if the duty in fact arises independently of that contract. Breach of contract occurs where that which is complained of is a breach of duty arising out of the obligations undertaken by the contract. If in order to make out a cause of action it is not necessary for the plaintiff to rely on a contract, a suit is one founded on tort; but on the other hand, if, in order successfully to maintain the suit, it is necessary for him to rely upon and prove a contract, the action is one founded upon contract. In the instant case, in order to make out a cause of action it was necessary for the respondent to rely on a contract. The accusations and counter-accusations by both parties are of negligent acts and omissions constituting breach of duties arising under contract and therefore this is an action in contract rather than tort.

ii. <u>The extent of the bank's duty to protect a customer from fraud and crime at an ATM.</u>

[28] At common law, there is an obligation on a bank to comply with its customer's payment order so long as the account is in credit (see *Bank of New South Wales v. Laing [1954] AC 135)*. Banks are also entitled to reject a payment order where the customer has breached the agreed terms and conditions governing the account, for example by not providing two signatures for a joint account payment, or where making the payment would be considered unlawful. A bank will only have the authority to make a payment or debit a customer's account if it can show that authority has been obtained from the customer. The form and procedure for giving consent to the execution of a transaction must have been set out in the information given to a customer before a transaction is concluded.

[29] In the context of digital banking, authority of the customer is controlled by the restricted personal access to his or her PIN which he or she has duty to keep secret. Upon slotting of the correct card and typing of the corresponding PIN onto

the machine's keypad, the bank is deemed to have received the necessary authorisation from the customer and then the ATM dispenses cash, which makes bank customers easy targets for thieves and fraudsters, thus rendering this method of payment risky. As a result, if a third party were to gain access to a customer's electronic payment device or were able to bypass it altogether and send payment instructions to a bank, the obligation on the bank to assess whether it had the consent to process the transaction would be dependent on the terms of the contract between the parties.

[30] For the criminal or fraudster, there are three options for illicit access to cash at the ATM: copying the card, stealing the card or going directly for the cash by breaking into the machine or snatching it from a customer who has just withdrawn it from the machine. Of course, to be effective in terms of accessing cash via the ATM, the first two options must also involve theft of the PIN. It was contended by Counsel for the respondent, and indeed the trial Court agreed and found that, the fraud committed in the instant case could have been prevented had there been a security guard at the time. Whereas it is easy to conceive of situations where a security guard may thwart or foil an attempted or planned theft of cash by breakage into the machine itself, or by snatching it from a customer who has just withdrawn cash from the machine, the possibility of prevention by a security guard, of unauthorised access to, or theft of, both the card and the PIN from a customer while at the ATM, requires a closer examination.

a) <u>Liability for third party fraud and insider bank-employee facilitated fraud</u>.

[31] Criminals have been known to copy information off the ATM Card magnetic strip by attaching card skimming devices to the fascia of an ATM (see *Kornark Investments (U) Ltd v. Stanbic Bank Uganda Ltd, H.C. Civil Suit No. 116 of 2010; Mars Tours and Travel Ltd v. Stanbic Bank Ltd, H. C. Civil Suit No. 120 of 2010; Ivan Gachev and two others v. Uganda, C.A. Criminal Appeal No. 155 of 2013 and*

Best Connect Tours and Travel (U) Ltd v. Stanbic Bank Ltd H.C. Civil Suit No. 172 of 2010). A genuine bank card's magnetic-stripe is copied and then placed on a duplicate card. This cloned card can then be used to withdraw money from an ATM. However, the fraudster will not be able make any withdrawals unless he has also obtained the PIN. 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.

[32] Among the other methods used by criminals is card trapping (where the criminal steals the actual card at the ATM) whether it be a magnetic stripe card or a smart card. The criminal does this by attaching a device to the card reader slot that allows the card to be inserted in the normal way but stops the card from being returned to the cardholder. Sometimes this activity is compounded by the criminal, in the guise of offering assistance, advising the cardholder to re-enter the PIN (which is observed). When the cardholder gives up and walks away the criminal will release the device with the card. This is often combined with other techniques such as fitting a tiny camera over the ATM keypad to record the victim's PIN so it can be used to authorise fraudulent transactions.

[33] Another scenario could be, fraudsters targeting old age persons or those persons who are not tech savvy. Most of the time what happens with such persons inside an ATM booth is, they face difficulty in withdrawing cash and require assistance, hence becoming soft targets of the fraudsters. The fraudsters carry a number of ATM cards of various banks (most probably stolen from other bank users) and when they spot a soft target in operating the ATM they offer them help. They ask for the user's ATM pin and help them in his task. But during this so called help they replace the ATM card of the user with another card of the same bank. After a period of time, when the fraudster makes transaction from the user's card, the user realises that money has been withdrawn from his bank account. Further, it is usually when the user attempts to use the card or approaches the bank to report

the incident, then he comes to know that he is not in possession of his own ATM card and his ATM card has been swapped by a criminal.

[34] Another modus operandi of the defrauders involves jamming both the “Enter” and “Cancel” buttons on the ATM machine by applying glue or by inserting a pin or blade at the edge of the button. So when the customer tries to press the “Enter/OK” button after entering his ATM PIN, the key does not function and the customer cannot proceed with his transaction. At this juncture the customer thinks that the machine is not working and tries to cancel the transaction, which also does not go through as that button is also jammed. Thinking that the transaction is cancelled, he leaves the ATM machine. As soon as the customer leaves or is prompted to visit the nearby ATM machine, the fraudster takes over the machine and since the transaction is active for around 30 seconds in most cases (some banks have reduced it to 20 seconds), he keeps the transaction active by pressing some functional buttons and in the meantime removes the glue or pin from the “Enter” button to go ahead with the transaction. The fraudster then withdraws the cash from the customer’s account, leaving the customer unaware of the fraud till he checks the message from the bank.

[35] Yet another form of ATM-related fraud that has come to banks’ notice is card swapping. When a customer visits an ATM and uses his/her card for a transaction, a stranger pretending to offer help (fraudster) notes down the ATM PIN when it is keyed in by the customer. Later, while returning the card to the customer, the stranger swaps the customer’s card with a dummy card that is identical to the customer’s card. Since the customer is unaware of the swapping, he secures the dummy card whereas the fraudster gets both the card and the PIN which he uses to withdraw cash till the card is blocked by the customer. Experts say that the fraudsters keep several dummy cards of various banks and depending upon the card provided by the customer for the transaction, they pull out a similar card and hand it over to the customer. Since most customers don’t check if the returned card is theirs or not, the fraudsters are successful in cheating the customer.

[36] Innumerable ways and means are adopted by the fraudsters. Electronic banking systems fraud is constantly evolving as criminals discover new ways to thwart the efforts of financial institutions and other interested parties to protect transaction data. Indeed, the techniques employed by fraudsters are numerous and are adapted to overcome new protection measures. There is no single solution that will eliminate fraud. Protecting customers from fraud and Cyber-attacks requires staying ahead of fraudsters and cyber-criminals. It becomes essential to not only identify gaps and breaches, but also fill them before a single incident takes place. Owing to the challenge of balancing security and usability for users as well as business needs, banks have relied on a multitude of different security solutions and authentication mechanisms, with approaches changing over time to meet security needs and reduce cybercrime losses. The bank may introduce new security features in the digital system such as software upgrades to prevent frauds of this type. They may, for example, make use of digital certificates and strong encryption which in essence reduces the risks of card information being abused. Other countermeasures include consumer awareness messaging. It follows that the bank and its customer must use complementary countermeasures to thwart criminal activity at the ATM.

[37] It is trite that Banks owe a duty of care to users of their payment technology to provide sufficient features to ensure that information transmitted on their electronic platform is protected from fraudsters. Evidence must therefore be led to reveal avoidable gaps in the payment technology system which leaves it vulnerable to fraudsters. In general terms, the bank will be liable when the unauthorised transaction takes place in circumstances of contributory fraud/negligence/deficiency on the part of bank, or third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, and the customer notifies the bank within a reasonable time of receiving the communication from the bank regarding the unauthorised transaction, or when

it fails to ensure sufficient security to prevent fraudsters from accessing the technology behind its electronic payment system.

[38] For ensuring safety and security of electronic banking transactions carried out by the customers, the bank should; have in place digital or other systems capable of analysing / monitoring transactions to identify suspicious ones; monitor the network regularly to check authenticity of source of transactions; SMS alerts are sent to customers for every electronic banking transaction carried out by them; regular risk assessment and analyses of the system are undertaken, and also whenever the situation demands; regularly conduct awareness programme on carrying out safe electronic banking transactions to its customers and staff; repeatedly advise its customers about the risks and responsibilities involved in electronic banking transactions by various means.

[39] The common law principle is that a bank has an obligation to exercise reasonable care and skill in performing their mandate. What this means in matters of electronic transactions is that banks have a duty to take reasonable measures to ensure that their digital banking systems are secure and are regularly reviewed and updated. This requires constant testing, artificial simulations, and machine learning at the back-end. They should know when a suspicious transaction or withdrawal takes place, and to this extent, must ensure that transactions on their digital banking services and received by their systems can be checked and traced. A bank will not be held liable once it shows that the security procedure it has in place is a commercially reasonable method of providing security against unauthorised digital payment orders.

[40] In contrast, the bank will be liable where its employee colludes with fraudsters outside the bank in appropriating the holder's card and PIN and for fraud perpetrated by the bank employees who have access to sensitive customer information. Banks are under a duty to observe highest standards of integrity and performance (see *Makau Nairuba Mabel v. Crane Bank Ltd H. C. Civil Suit No.*

380 of 2009). A bank employee with knowledge of circumstances which would indicate the facts to an honest and reasonable man or would put an honest and reasonable man on enquiry, acts with "knowing assistance" (see *Selangor United Rubber Estates Ltd v Cradock (No.3) [1968] 1 WLR 1555 at 1590* and *Baden Delvaux v. Société Générale [1992] All ER 161 at 235)*. A bank employee dishonestly assists in a transaction if they have sufficient knowledge to render their participation in the transaction contrary to normally acceptable standards of honest conduct thereby rendering "dishonest assistance" (see *Barlow Clowes International Ltd v. Eurotrust International Ltd [2005] UKPC 37; [2006] 1 WLR 1476, para 15 per Lord Hoffmann).* Although the dishonest assister will often know that what he or she is doing is dishonest, that subjective understanding is not necessary. Deliberately closing one's eyes, in the sense of having suspicions of misfeasance but making a conscious decision not to ask questions or otherwise enquire, satisfies the test of dishonesty (see *Royal Brunei Airlines Snd Bhd v. Tan [1995] 2 AC 378, 389E-F per Lord Nicholls of Birkenhead).*

b) Safety from violent attacks and the invasion of personal space.

[41] Generally the law does not impose a duty to protect from the intentional criminal acts of third parties. At common law, a private person or corporation, as distinguished from governmental units, has no duty whatsoever to protect others from the criminal acts of third parties. However, special relationships and special circumstances may combine to impose liability. Unless expressly excluded by the contract, banks will generally owe a parallel common law duty of care to customers in tort (often but not necessarily consistent with the express contractual terms) to take reasonable care in relation to the services they provide. The current approach of the courts, when considering the scope of the duty of care assumed by banks at their facilities, is to look at the foreseeability of the risk involved and then consider whether the loss suffered flowed as a result of that specific risk in fact coming to pass.

[42] Although as a general rule, there is no duty imposed upon a property owner to protect others from criminal attacks by third persons on his property, however, when there exists a special relationship between the parties, such as business inviter and invitee, the law may impose a duty to protect from reasonably foreseeable criminal activity. Exceptionally therefore, a duty may be imposed on a property owner to take reasonable precautions to protect invitees from criminal attack, where the property owner possessed actual or constructive knowledge that criminal activity which could endanger an invitee was a probability.

[43] Commercial establishments are subject to varying degrees of criminal attack. The common law rule regarding a commercial property owner and an invitee is that an occupant or owner of premises owes to an invitee a duty to use ordinary care to have the premises in a reasonably safe condition for use in a manner consistent with the purpose of the invitation, not to lead such person into a dangerous trap and to give such person adequate and timely notice and warning of latent or concealed perils which are known to the owner but not to the invitee. Under this rule, the knowledge of the property owner regarding the danger on his land is relevant. It is not, however, the only factor to be considered. Also relevant is the invitee's knowledge. An inviter will not be liable for criminal attacks by a third party unless he is aware of a danger of which his invitee is unaware.

[44] The duty of a property owners with respect to criminal acts cannot be equated with their duty with respect to careless or negligent acts. If the owner is to be held liable for the sudden criminal acts of third persons, there must be a showing that the owner was on notice in some manner of the imminent probability of the act. A possessor of property who holds it open to the public for entry for his business purposes, whose mode of operation of his premises does not attract or provide a climate for crime, has no duty to guard against the criminal acts of a third party, unless he knows or has reason to know that acts are occurring or about to occur on the premises that pose imminent probability of harm to an invitee; whereupon a duty of reasonable care to protect against such act arises. In such cases a duty

is owed to members of the public while they are upon the property for such a purpose, by the possessor to exercise reasonable care to (a) discover that such acts are being done or are likely to be done, or (b) give a warning adequate to enable the visitors to avoid the harm, or otherwise to protect them against it. In determining whether a duty exists, reasonable foreseeability of harm is the primary concern. The fact that a person using an ATM might be subject to fraud is conceivable, but conceivability is not the equivalent of foreseeability.

[45] Banks are responsible for keeping customers safe while on their property. Banks know that ATMs are common targets of crime, so they must provide adequate security at and around the machines to keep their customers safe. Since crimes perpetrated against ATM customers occur on bank property, ATM owners are required to provide customers with adequate security measures. Bank owners are responsible for gauging the risk of crime and using proper security measures to prevent harm to customers; at least one camera inside the machine pointing out; adequate lighting around the ATM; should not have plants, pillars, shrubbery, or other large items nearby that criminals could hide behind; ensure that access to the machines is always limited to persons possessing valid ATM cards; and security personnel that ensure the safety of ATM users.

[46] One of the reasons behind the ability of fraudsters accessing ATM machines and successfully installing “skimming machines” and “spy cameras” is mostly because of lack of security at the ATM booths. Also, the fraudsters initially conduct reconnaissance and select those ATM booths where security is at a weak point. This is a more technical mode of duping and the cardholder can hardly do anything about it as the miscreants plant a small skimming device in the card slot of the ATM machine and it can read the magnetic tape information of the card when the card goes through the skimming device. With the copied magnetic information, the defrauder can reproduce a duplicate card (on any plastic card) to be used later to withdraw cash. In order to access the PIN, the fraudster also installs a small camera at the ATM kiosk that can capture the ATM pin when it is entered by the

cardholder. One of the ideas behind visible security personnel and devices is that many potential criminals will not attempt criminal activity if there is a high probability that they will be apprehended in the process.

[47] The issue then is whether the appellant as the owner of the ATM at its "Metro Branch," located on the NSSF Building along Kampala Road, had a duty to take reasonable precautions to secure its premises against violent attacks. In determining whether a duty exists, reasonable foreseeability of harm is the primary concern. The duty attaches if the appellant knew or had reason to know from past experience that there was a likelihood of conduct on the part of third parties, which was likely to endanger the safety of users of the ATM. Although as a general rule, there is no duty on a landowner to protect others from criminal attacks by third persons while on his or her property, when there exists a special relationship between the parties, such as business invitor and invitee, the law may impose a duty to protect from reasonably foreseeable criminal activity. The relationship between a bank and an ATM customer is that of business invitor-invitee and qualifies as a special relationship requiring a duty to protect invitees against foreseeable violent crime.

[48] A business owner who has notice of prior criminal violent attacks occurring on his or her property has a duty to protect its customers and business invitees, from such attacks. However, generalised allegations of crime will not suffice to establish that future criminal attacks are foreseeable. For example in a case where the plaintiff based her claim of foreseeability on allegations that 1,500 to 5,000 criminal attacks on ATM customers occurred annually nationwide, but had no evidence of any such attacks having previously occurred at the particular ATM in issue and was unable to make assertions regarding specific locations or specific times at which future crimes may occur, the Court found that that plaintiff has not sufficiently alleged that future attacks were foreseeable so as to give rise to a duty on the part of defendants to protect from such attacks (*see Popp v. Cash Station, Inc., 244 Ill. App. 3d 87).*

[49] The loss that was sustained in the instant case was not perpetrated by way of a violent attack while the respondent was at the ATM. There was equally no evidence of a history of such attacks such as would have rendered future attacks foreseeable so as to give rise to a duty on the part of appellant to protect the respondent from such attacks by securing the ATM. The absence of security guards would therefore be immaterial for that purpose. The respondent's case instead was that on basis of the appellant having published on its official website, information providing tips to customers on how to prevent such fraud at ATMS generally, future attacks of a similar nature were foreseeable at the appellant's "Metro Branch" ATM so as to give rise to a duty on the part of appellant to protect him from such attacks by stationing private security guards at the location.

[50] This argument is flawed for two reasons; in the first place such a duty is founded on reasonable, not speculative, foreseeability. The reasonable foreseeability inquiry is objective (i.e. into what reasonably ought to have been foreseen), and it must be undertaken from the standpoint of a reasonable person. In cases of breach of contract, courts assess foreseeability, as awareness of possible future occurrences, from the time a contract was made, not at the time of the breach. An objective, reasonable-person-in-the-circumstances standard is used, because the purpose of damages is to protect only the reasonable expectation interest of the injured party. Courts consider if the party at fault had adequate knowledge about the specifics of their situation, that they could have foreseen the probability of damages. As for the subjective facts that can expand liability beyond the objective constraint, they are measured by what the breaching party "had reason to know" at the time the contract was made. The inquiry is into information actually available to the breaching party (although there is an objective component, in that the subjective facts must be interpreted as they would have been understood by a reasonable person in the circumstances).

[51] By enacting *The Anti–Money Laundering Act, 2013*, Parliament clearly never intended to create a private right of action for citizens injured by a failure to perform

the "know your customer" obligations. The fact that the checks required by the "know your customer" obligations under the Act may have a deterrent effect on would-be fraudsters, is not enough in itself to create a private law right of action under the Act for the benefit of third parties (see *X (Minors) v. Bedfordshire County Council [1995] 2 AC 633 at p 731* and *P & P Property Ltd v. Owen, White & Catlin LLP [2018] EWCA 1082; [2019] Ch 273; [2018] 3 WLR 1244*). The Act has no direct application in deciding who, amongst a number of innocent victims of the imposter's fraud, should bear the loss.

[52] In the circumstances of this case, there is no evidence to show that it was reasonably in the contemplation of the parties at the time the respondent subscribed for the appellant's ATM services that the appellant was as well offering the respondent protection from all manner of fraudulent schemes that may be perpetrated by third parties at the appellant's ATMs. For such a duty to arise, at a minimum, evidence would be required to show that at the time of the contract, the appellant had notice of prior criminal incidents of a similar type related to the bank's ATMs, in order to establish a basis for the argument that future attacks of a similar nature were foreseeable. The Court should determine whether there were a sufficient number of prior incidents, whether the prior incidents were sufficiently similar, or whether the prior incidents were on or close enough in proximity to the bank installations to make the ATM crime in issue foreseeable at the time. The Court below did not have such evidence before it. To the contrary, D.W.1 Ms. Faith Amongi specifically testified at page 61 of the record of appeal, that "the bank had never received information of fraudsters taking advantage of customers.

[53] Secondly, a private security guard is responsible first and foremost for the safety of the property of the company or group that he or she has been hired to protect, in this case the ATM, which involves monitoring access in and out of the booths, as well as responding to incidents, security threats, and emergency situations. Their job is to observe and report. When something illegal happens then they alert the police. Private security guards often rely on their visible presence to deter

potential threats. By patrolling or standing watch, they create a sense of security and discourage unwanted activities. A security guard represents the ATM owner and has the authority to ask anyone to leave if there is a violation of policy. In certain situations, where there is an imminent threat to the safety of individuals or property, security guards may intervene and de-escalate situations, or use physical restraint techniques to immobilise or control individuals. They may also provide assistance to individuals in need, such as helping with directions.

[54] Private security guards are the first, but certainly not the ultimate, line of defence against fraudsters or violent attacks for ATM users within the vicinity of its location. They are not deployed to provide personal or close protection for the ATM users. Even if they were, often one of the most challenging aspects of personal or close protection can be balancing the customer's need for personal space while at the ATM, with the security related functions of the job. ATM users can have their very specific personal preferences, including having their personal helpers with them inside the booth during their transactions. A close protection security officer can often be a seemly intrusive inconvenience to the uninitiated ATM user in such situations. They are not expected to hover over the customer while they are transacting at the ATM. They are expected to respect the privacy rights of individuals at the ATM. Utmost professionalism and constraint would be expected so as not to embarrass the customer in any way. It is important for the private security guards to remain especially flexible and adaptable in these situations.

[55] Personal space can be considered a boundary within which one feels comfortable. What feels too close for comfort for some ATM users might be acceptable for others. Considering that the concept of personal space is subjective, it follows therefore that it is the customers' duty to manage their personal space by preventing invasions of that space in a manner which causes an experience of physical or emotional discomfort, and to bring such invasions, when they occur, to the immediate attention of the private security guards deployed at the ATM. Personal space is like an invisible bubble that surrounds the individual, providing

a sense of security and control over one's immediate environment. The guards would always need to be in close enough proximity, but without intrusion into that personal space, to instantly respond in such emergencies.

[56] While waiting in line or inside the ATM booth itself, the customer must make sure he or she has adequate personal space. The customer must keep an eye out for anyone standing too close while they are conducting their transaction. The customer must be cautious of people who might be trying to watch him or her enter the PIN. Shoulder surfing happens when a stranger furtively views the ATM screen and keypad to obtain personal information. It is one of the few attack methods that requires the attacker to be in close proximity to the ATM user. It is the duty of the customer to pay attention to his or her surroundings at that critical time while accessing private information, which usually takes only a few moments. It does not require one to be on the constant look-out throughout the transaction as suggested by the Court below. Shoulder surfers cannot steal what they can't see. The customer should position his or her body between their sensitive information and anyone's direct line of sight. For example, by shielding the keys on a PIN pad when entering it. Upon detecting that their sensitive information has been compromised, they have a duty to report it to the bank in order to take back control of their accounts.

iii. <u>The bank customer's duty to prevent fraud.</u>

[57] ATMs have become an integral part of society's daily lives, providing bank customers with quick and convenient access to their hard-earned cash. However, the convenience of ATMs also presents security risks, making it essential for anyone to take steps to protect themselves while using these machines. Although the average bank customer is not expected to be constantly alert to the possibility of fraud taking place at the ATM, and bank customers are not reasonably expected to be extra vigilant and to react at a moment's notice to any potential fraud taking

place on their accounts, however, there are some reasonable expectations placed on the customer.

[58] In terms of digital banking, the customer's common law duty to effect the payment order with reasonable care so as to limit the chances of fraud and deception, imposes a number of a number of obligations in terms of securing their transactions. Selecting a well-lit, busy, and reputable ATM location is a customer's first line of defence. A customer is expected to avoid using ATMs in isolated or poorly maintained areas, as they are more vulnerable to criminal activity. The customer has the duty to use the ATM card in accordance with its terms and conditions, to take all reasonable steps to keep the card's security features safe, and to inform the bank, without undue delay, on becoming aware of its loss, theft, misappropriation or unauthorised use.

[59] At the ATM booth, the customer must ensure: he or she conducts all ATM transactions in complete privacy by using the hands or body to obscure the keypad from prying eyes or hidden cameras, and by not seeking or receiving help from any unknown person. The customer should never let anyone see him or her entering their Personal Identification Number. The customer should not to hand over his or her ATM card to any unknown person and especially where that person's activities at the machine are not in the customer's line of sight and also ensure that the transaction is cancelled, before they leave the machine to be accessed by someone else. After completion of transaction, he or she should ensure that the "welcome screen" is displayed on the ATM. The customer should ensure that his or her card is always in his or her eyesight while at the ATM. The ATM card and PIN must be protected as if it were cash. The customer should not share his or her ATM card details with any unknown person, or even the bank officials or its agents. The customer should beware of and alert to suspicious movements of people around the ATM or strangers trying to engage him or her in conversation, or offering unsolicited help.

[60] The bank must produce substantial evidence or argument that the card holder was negligent and is therefore responsible for the losses incurred. The customer will be liable for the loss occurring due to unauthorised transactions in the following cases; where the loss is due to negligence by a customer, such as where he or she has shared the payment credentials details namely; internet banking user id /PIN, ATM Card PIN/OTP or due to improper protection on customer devices like mobile phones/laptops/desktops leading to malware/Trojan or phishing/vishing attacks. Similarly, they are liable for loss arising from phantom withdrawals. These are a cases where it is suspected that a person known or close to the card holder accessed the card and knowing the PIN, makes 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.

[61] For losses caused by unauthorised third party action where the cause, gap or deficiency lies neither with the bank nor with the customer but lies elsewhere, and the customer notifies the bank within a reasonable time of detecting the unauthorised transaction, or when the customer fails to ensure sufficient security to prevent fraudsters from accessing the bank's technology behind its electronic payment system, the customer bears the entire loss incurred until he or she reports the unauthorised transaction to the bank. Any loss occurring after the reporting of the unauthorised transaction is borne by the bank.

iv. <u>Attribution of liability based on the facts of the case.</u>

[62] In order to attribute liability for this loss, conclusions must be drawn first as to what actually happened based on the probabilities. The process begins by elimination systemic failures, glitches or lapses in the appellant's electronic system. Also ruled out is loss through violent attack or assault while at the ATM. What is left is a determination of the type of third party fraud that was perpetrated. It is not in doubt

that it was as a result of a fraudster's action of obtaining unauthorised access to the respondent's ATM card. The mechanism used did not involve cloning. 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, which was not the case here. The modus operandi of the fraudster who victimised the respondent apparently was of the "stranger pretending to offer help" type followed by a card swapping. In his own testimony, the respondent admitted he was having some difficulty when he stated "as a senior citizen who reads with glasses, I had to go very close…it was not my first time to use the card for deposit but at [this] particular branch it was the first time to try to use it for deposit."

[63] The respondent's account of the sequence of events differed in significant aspects from that of the appellant regarding what the proximate cause of access to the respondent's ATM card and PIN was. The respondent contended it was that as he drew closer to read the information on the screen, "I saw a hand pass by my shoulder and pressed a button and the card came out. I didn't alert the security because it was uncalled for at the time…..I didn't solicit any help while at the machine. I am literate and this person was actually an intruder. There was no security guard at the ATM and the security people were at the main entry." P.W.2 No. 58277 Tumwesigye Daniel testified that the ATM booth was large enough to admit two of three customers at a time, and it contained two ATM machines. From his recollection upon viewing the cctv footage, the respondent "didn't protest when the stranger came to assist him in the ATM. The stranger went into the ATM, tried to interact with the plaintiff, though I did not hear what they talked about but it was very clear he was trying to offer help. The stranger later left the ATM room holding something in his hand. The plaintiff remained at the ATM…..I fund that there is security at the bank entrance and inside the bank. There was no security at the ATM entrance and inside. THE bank entrance and the ATM entrance is different. When the stranger approached and entered ….. the stranger touched the plaintiff a bit and then entered and started talking to the plaintiff."

[64] The appellant's version as given by D.W.1 Ms. Faith Amongi who testified; "it is on the same day when the card had been retrieved that I realised his card had bene swapped. It is when he came to pick it after I had called him that same day…the ATM area is also at the same location. The ATM is outside the bank, not inside. To access it you use a different entrance, not the same as the bank's….. There are security personnel at the bank…. The cctv footage showed the card was swapped at the bank premises. The plaintiff notified me of his card being captured, not the fraudulent withdrawals ……There should be security guards at the ATM. I cannot remember for sure whether there were any that day…… the owner of the card should keep their PIN safe at the machine and point of sale and one should be expected to cover their PIN number. This information is given to customers regarding covering of their PINs while at the ATM transacting…..the plaintiff kind of hand a conversation for some minutes with the fraudster as per the footage, the person behind entered the machine (sic)…..the fraudster withdrew a sum of shs. 5,710,000= from the respondent's account in twelve instalments all on the same day, 19th March, 2021 between 10:47 am and 11:52 am via the DFCU Bank ATM at Nandos (five withdrawals whiten a space of five minutes, the last one of which was at 10:52 am), and the ABSA Bank Point of sale at Dalton (U) Ltd (seven payments within a period of thirty-seven minutes, the first one of which was at 11:15 am). By the time the plaintiff notified the bank about the incident at the ATM, the above amounts had already been withdrawn from the plaintiff's bank account using his debit card. Some of the transactions were reflected on the plaintiff's bank statement after19th March, 2021 because the alleged unknown person used the plaintiff's card at other banks. ATMs and / or points of sale. The transactions reflected onto the plaintiff's bank stamen after reconciliation with Visa….What happens when a card is used at another ATM or a point of sale, the reconciliation isn't done immediately. Sometimes it can take a day ow two for the transaction to go through fully….when the transaction is initiated, the customer gets the money that day the transaction is concluded but the reconciliation is done later."

[65] It is for the Court to resolve the differences between these two versions, through a process of evaluation. What emerges from the two versions is that the ATM in issue is in close proximity of the appellant's branch, in fact located on the same building that houses the appellant's "Metro Branch," except that the entrance to the banking hall and that to the ATM are different. Although there was no security guard at the entrance to the ATM, in view of the proximity of the two entrances to each other, the ones at the entrance to the banking hall would reasonably be expected to make a timely response to any emergency occurring at the ATM, if brought to their attention. It would seem that on the fateful morning no particular security guard had been deployed to monitor and control access to the ATM booth. This though is insignificant in light of the fact that that the booth contained two ATMs and the simultaneous access by more than one person would not be unusual nor would it have placed such a security guard on alert.

[66] Where a security breach occurs at the ATM, the onus lies on the customer to prove negligence by showing that the bank in question could have done more to safeguard the integrity of customer's personal information from unauthorised access, and that the bank failed to put in place effective counter fraud measures to safeguard that sensitive information. This includes personal banking details such as an account name, account number and personal identification numbers or codes which can be used to access a customer's account to perpetrate fraud, as well as any information about the customer that has been acquired by the bank.

[67] With the increasing sophistication of scams, the bar for gross negligence is high; it is more than just mere carelessness. A person can commit gross negligence if they intentionally act in a manner that they know, or should know, is highly likely to cause them loss. It involves a failure to use even slight care or conduct that is so careless as to show complete disregard for the safety of the card's security features and their Personal Identification Number. Factors that will be relevant to the degree of negligence include the complexity of the scam and whether the customer can reasonably be expected to have paused or otherwise prevented the

fraud from being executed. One of the key things to be considered is the environment that was created by the fraudster for the consumer, essentially the nature of the "spell that was cast." At the time of requesting the appellant to increase his Debit Card daily default withdrawal limit from shs. 2,000,000/= to shs. 5,000,000/= the respondent signed an indemnity document dated 29th January, 2018 (exhibit D. Ex.1) containing the following pertinent clauses;

> The Bank has accepted to grant my request provided it receives a release an indemnity in the form hereof. I am prepared to give such release and indemnity by signing this document.
>
> 1. That I am aware of the risks involved in Debit Card/Internet Banking transactions,
> 2. …..
> 3. ……
> 4. That I am fully responsible for the safe keeping and proper use of my Debit Card/Internet Banking personalised identification number/password, (tick and initial applicable option),
> 5. That the bank will not be liable for any loss or damage I may suffer in excess of the daily default withdrawal limit whatever the cause of such loss or damage.

[68] Attached to the indemnity document is a set of terms and conditions of Auto Bank/Debit Card (exhibit D. Ex.2) containing the following pertinent clauses;

> 3. Use of the Card
> 3.1 You must only use the card yourself and must not allow any other person to use the card.
> 5. Use of the Card
> 5.1 You are responsible for the safe keeping and proper use of the card. You must either memorise the PIN the Bank supplies, or keep any record of the PIN separate from the card and in a safe place.
> 5.2 As soon as you discover or suspect that your card is lost or stolen or your PIN is compromised, you must notify the Bank immediately by telephone. The Bank will stop

the card as soon as reasonably possible after such notification. Delay in notifying the Bank will be considered as negligence on your part.

5.3 If you are negligent in not promptly reporting the card lost or stolen, you will be responsible for all cash drawn including where the PIN is used to withdraw money or for payment of goods and services bought with the card, before the Bank has stopped the card.

[69] This is the parties' agreed allocation of risk of fraud. The distinction between transactions taking place before notification of loss, theft or misappropriation of the ATM card and transactions taking place after notification is a crucial provision for dividing liability in the case when the transaction is unauthorised. The implication of these indemnity obligations is that where the respondent's failure to exercise ordinary care in safeguarding his personalised identification number causes or substantially contributes to unauthorised access to his funds by use of the debit card issued to him, thereby occasioning him loss or injury, he cannot use his lack of authorisation of the withdrawal as a basis for a claim for refund against the appellant. The same applies to the respondent's delay in reporting the card as lost. The respondent bears the losses deriving from the use of a lost or stolen ATM card or, if he has failed to keep the personalised security features safe from misappropriation, occurring before he has fulfilled his obligation to notify the appellant.

[70] From the evacuation of the evidence adduced by the parties, it is evident that the respondent did not by word or conduct, express any indignation toward the invasion of his private space when the intruder reached out across his shoulder. Indeed he instead appeared to have acquiesced in it by not protesting the stranger's having touched the keypad before he had concluded his transaction. He also did not call the occurrence of this to the attention of the security guards at the entrance to the banking hall. In his own words, he did not "alert the security guards because it was uncalled for at the time." That the respondent's sensitive data was accessed by an unauthorised third party while at the ATM is directly attributable to

his failure to manage his personal space at the ATM. By his failure to protest when unsolicited help came from a stranger while at the ATM and to prevent that person from seeing him entering his Personal Identification Number, the respondent's conduct fell short of the conduct demanded of a reasonable customer at an ATM. He should have been concerned and watchful as he typed his PIN. In these circumstances the respondent's negligence is the real, immediate or proximate cause of the loss occasioned by the fraud.

[71] The learned trial Magistrate not only misdirected herself on the contractual allocation of risk of loss agreed to by the parties, but she also wrongly attributed the loss to the absence of security guards at the ATM as the proximate cause of the loss. She further misdirected herself when she rejected the appellant's evidence to the effect that the card had been blocked sometime after midday on 19th March, 2021 when the bank realised the respondent's card had ben swapped and instead found that withdrawal continued to be made from the respondent's account. Had she properly directed on the evidence adduced reading the processing of transactions where funds are withdrawn from ATMs of banks other than the one that issued the card in issue. Had she done so, she would have discovered that the respondent's bank statement (exhibit P. Ex. J) is a reflection of the postings made after reconciliation, not in real time of the withdrawal.

[72] According to clause 5.3 of the terms and conditions of Auto Bank/Debit Card, the appellant bears the financial consequences which occur after notification about a lost, stolen or misappropriated ATM Card. In the instant case, discovery of the fact that the respondent's card had been swapped was some time after midday on 19th March, 2021, yet the fraudster had made the final withdrawal by way of payment at the ABSA Bank Point of sale at Dalton (U) Ltd at 11:52:06 whereupon the appellant blocked the card. No further withdrawals were made after the bank realised the respondent's card had been swapped that would have rendered the appellant liable under that contractual provision. By the time the respondent lodged

a formal notification, it was too late. Whether the appellant was actually able to prevent further use of the card is irrelevant in this case.

[73] It is for those reasons that the appeal succeeds on all grounds and is accordingly allowed. Consequently, the judgment of the court below is hereby set aside and instead judgment entered for the appellant against the respondent dismissing the suit. The costs of this appeal and of the court below are awarded to the appellant.

Delivered electronically this 12th day of January, 2024 ……Stephen Mubiru……

Stephen Mubiru
Judge,
12th January, 2024.

Appearances

For the appellant : M/s J, B, Byamugisha Advocates

For the respondent : M/s Nabukenya, Mulalira & Co. Advocates