THE REPUBLIC OF UGANDA

IN THE HIGH COURT OF UGANDA SITTING AT KAMPALA

(COMMERCIAL DIVISION)

CIVIL SUIT No. 0754 OF 2020

AIDA ATIKU …… PLAINTIFF

VERSUS

CENTENARY RURAL DEVELOPMENT BANK LIMITED …… DEFENDANT

Before: Hon Justice Stephen Mubiru.

JUDGMENT

a. The plaintiffs' claim;

The plaintiff sued the defendant seeking recovery of shs. 55,616,000/= claimed to have been negligently debited from her bank account with the defendant, general damages for breach of fiduciary duty, interest and costs. The plaintiff's claim is that on 2nd January, 2020 she opened up a personal savings account at the defendant's branch along Namirembe Road in Kampala. Between 4th and 10th January, 2020 the plaintiff deposited a total of shs. 56,320,000/= onto the said account. The plaintiff thereafter made only one withdrawal in the sum of shs. 700,000/= on 13th January, 2020. When she subsequently went to the bank on 27th August, 2020 to withdraw the rest of the amount intending to use it for the purchase of land, she was shocked to learn that her account had zero balance. She was informed by the bank staff that someone had over time been withdrawing diverse sums of money electronically from the account using the "CenteMobile" platform, yet she had never applied for such a service. She therefore demanded for a refund of her money, to no avail, hence the suit where she contends that the defendant was negligent.

b. The defence to the claim;

In its written statement of defence, the defendant denied the claim. It contended that although the plaintiff indeed opened up the said account and made the deposit pleaded, at the opening of the account she registered for the "CenteMobile" service offered by the bank. The plaintiff thereafter undertook multiple transactions though that platform. At all material time, the said transactions

were initiated and concluded using the plaintiff's officially registered mobile phone number. The defendant was never fraudulent nor negligent in any of the said transactions.

c. <u>The issues to be decided</u>;

In their joint memorandum of scheduling, the parties agreed on following issues for determination by court, namely;

1. Whether or not the plaintiff's account was fraudulently and / or negligently debited by the defendant.
2. Whether or not the defendant is liable for the fraudulent and / or negligent withdrawals made on the plaintiff's account.
3. What are the remedies available to the parties?

d. <u>The submissions of counsel for the plaintiff;</u>

M/s Kalende and Co. Advocates, counsel for the plaintiffs, submitted that when the plaintiff signed the application form on 2nd January, 2020 for opening up an account with the defendant, she was unaware that it contained provision for the "CenteMobile" service and for the provision of an ATM card. The content of the application form was never explained to her. The defendant failed in its duty of care it owed the plaintiff to explain to her the range of services offered, including the charges and fees involved, in order to enable her make an informed decision. At no time did she lose her phone or give it to any other person, yet throughout all material time after the opening of that account she received only one sms alert concerning a deposit made on 4th January, 2020. There was no evidence adduced to shoe that she mandated the defendant to authorise any withdrawals from the account. The defendant was therefore negligent when it permitted the withdrawal of a total of shs. 56,616,000/= from the account without her authority. The plaintiff is therefore entitled to a refund of the entire sum. She is also entitled to general damages for the distress caused to her by the loss of her money intended for purchase of a house. She is entitled to an award of interest and costs as well.

e. The submissions of counsel for the defendant.

M/s S & L and Advocates, counsel for the defendant, submitted that when the plaintiff signed the application form on 2nd January, 2020 for opening up an account with the defendant, she also signed up for the "CenteMobile" service, by specifically signing against the part reserved for that request. In doing this, she was assisted by one of her daughters, the then 42 year old P.W.2 Mirembe Hadijah, whose presence at the time was primarily to assist the plaintiff read and fill in that application form. On diverse dates between the month of January, 2020 and May, 2020 she withdrew or permitted the withdrawal of a total of shs. 56,616,000/= using that service, by means of her mobile phone number 0773 710 077. All transactions were undertaken using the plaintiff's authorised phone number and USSD Code. The said withdrawals were thus enabled by the plaintiff and did not involve any fraud or negligence on the part of the defendant. Despite having received alerts of all transactions undertaken on her account, the plaintiff never reported to the defendant any of them to have been fraudulent. Although she claimed to have made a report to the police no corroborative evidence was adduced. If the withdrawals were unauthorised by the plaintiff as claimed, then they occurred due to her own negligence. She accordingly is not entitled to the remedies sought. The suit should be dismissed with costs.

f. The decision;

In all civil litigation, the burden of proof requires the plaintiff, who is the creditor, to prove to court on a balance of probability, the plaintiff's entitlement to the relief being sought. The plaintiff must prove each element of its claim, or cause of action, in order to recover. In other words, the initial burden of proof is on the plaintiff to show the court why the defendant liable for the relief claimed. Generally, the plaintiff in the instant suit must show: (i) the existence of a contract and its essential terms; ii) a breach of a duty imposed by the contract; and (ii) resultant damages. The first two issues raised by the parties being inter-related, they will for purposes of convenience and the avoidance of unnecessary repetition, be considered concurrently.

1st issue; whether or not the plaintiff's account was fraudulently and / or negligently debited by the defendant.

2nd issue; whether or not the defendant is liable for the fraudulent and / or negligent withdrawals made on the plaintiff's account.

It is common ground between the parties that on 2nd January, 2020 the plaintiff opened up a personal savings account at the defendant's branch along Namirembe Road in Kampala. On 4th January, 2020 she deposited a sum of shs. 9,000,000/= and an additional sum of shs. 47,000,000/= on 10th January, 2020 to make a total of shs. 56,320,000/= deposited onto the said account. The plaintiff thereafter on 13th January, 2020 made a withdrawal in the sum of shs. 700,000/= across the counter. On diverse days thereafter, a total of shs. 56,616,000/= was withdrawn electronically from the account by use "CenteMobile," an electronic internet based banking platform offered by the defendant, that enables its customers to transact and access banking services using their mobile phones or similar electronic devices, anywhere, anytime.

While the plaintiff contends she never requested for that service, never used it and never authorised any person to use it in accessing or withdrawing money from her bank account, the defendant contends that she indeed applied for the service, and used it or authorised someone to access or withdraw money from her account, or in the alternative, was negligent when she enabled unauthorised persons to do so. In support of her claim, the plaintiff happens to have relied on the account opening standard form, exhibit P. Ex.1. Attached thereto is another standard form containing a section headed, "CenteMobile SERVICES DECLARATION," which reads as follows;

> I hereby apply for CenteMobile services. I warrant that the information given above is true and complete and I authorise you to take any enquiries necessary in connection with this application. I accept and agree to be abound by the general terms and conditions of use. I agree and I am liable for all charges incurred through the use of this service. I hereby indemnify the Bank against all losses, which may occur as a result of my use of service. I understand that Centenary Bank reserves the right to decline this application without giving reasons.

Just like all other sections of the standard form relating to the Credit Reference Bureau, ATM cards, and "sms" alerts, this section of the standard form too was duly signed. In her testimony, whereas the plaintiff admitted having signed the form, she contended that due to her failing sight, it is her daughter P.W.2 Hadija Mirembe who read though the application form. The plaintiff signed the form without reading and her daughter did not read it to her. She was only told "sign here, sign there." There was no explanation of what she was signing. She was never told what "sms" alerts were. The ATM component was never explained. She did not expect an ATM card and does not have any. She was never invited to collect the ATM card. She was not aware that the form had a provision for "CenteMobile." She did not know "CenteMobile" by then. The "CenteMobile" function was never explained to her. The implications of the document and the various services were never explained to her. She was never asked the type and mode of phone she had. She was never asked to call any of her relatives to explain the contents of the form to her.

At common law, there is a duty on the signatory of a contract to make sure that he or she understands the terms and conditions before signing it. A signature on a contractual document or other written agreement, demonstrates that a party has read, understood and consents to the terms and conditions in a contract. A party to an agreement is thus bound by his or her signature, regardless of whether he or she has actually read the contract or not (see *L'Estrange v. F Graucob Limited [1934] 2 KB 394; [1934] All ER 16*). Exceptions to this rule apply in instances where the signature was obtained unfairly through misrepresentation, duress or undue influence, or where the text of a contract was so small that it is impossible to decipher, not even with a magnifying glass. The general rule therefore is that a party of full age and understanding is normally bound by his or her signature to a contractual document whether he or she reads it or understands it or not. Equity does not save people from the consequences of their own folly but will save them from being victimised by other people. Whenever a person of full age and understanding puts his or her signature to a legal document without taking the trouble of reading it or without asking the document to be read and explained to him or her but signs it relying on the word of another as to its character, content or effect, he or she cannot be heard to say that it is not his or her document.

Secondly, according to section 92 of *The Evidence Act*, when the terms of a contract have been proved by the production of the document itself, or secondary evidence of its contents in cases in

which secondary evidence is admissible, no evidence of any oral agreement or statement may be admitted, as between the parties to any such instrument or their representatives in interest, for the purpose of contradicting, varying, adding to or subtracting from its terms, unless there is evidence of fraud, duress, or a mutual mistake (see also *Evans v. Roe and others (1872) L. R. 7 C. P. 138; Halsbury's Laws of England* (4th edn.) vol. 9 (1) para 622; *Chitty on Contracts* 24th Edition Vol I page 338; *Jacob v. Batavia and General Plantations Trust, (1924)1 Ch. 287*; *Muthuuri v. National Industrial Credit Bank Ltd [2003] KLR 145*; and *Robin v. Gervon Berger Association Limited And Others [1986] WLR 526 at 530*).

In other words, any information leading up to or during a contract that is not included in writing is considered inadmissible evidence and is excluded (see *Bank of Australasia v. Palmer [1897] A. C. 540 at 545*). Terms in a writing intended by the parties as a final expression of their agreement may not be contradicted by evidence of any prior agreement or of a contemporaneous oral agreement but may be explained or supplemented by course of dealing, usage of trade, or by course of performance; and by evidence of consistent additional terms unless the court finds the writing to have been intended also as a complete and exclusive statement of the terms of the agreement. The parol evidence rule assumes that the formal writing reflects the parties' minds at a point of maximum resolution and, hence, that duties and restrictions that do not appear in the written document, even though apparently accepted an earlier stage, were not intended by the parties to survive (see Marvin A. Chirelstein, in *Concepts and Case Analysis in the Law of Contracts* (5th ed. 2006) at p 98).

If, however, a party has been misled in executing a contract or signing a document essentially different from that which he intended to execute or sign, he can plead *non est factum* in a suit against him and the contract or writing is completely void in whomsoever hands it may come. The doctrine of *non est factum* though does not apply unless there is a misrepresentation in inducing a mistaken belief as to the class of character of the supposed document and not a misrepresentation simply as to its contents. On the other hand, a mistake as to the contents of a deed of document is not sufficient (see *Saunders v. Anglia Building Society (sub nom Gallie v. Lee) [1971] AC 1004*). *Non est factum* applies where the person asserting it; (i) did not sign the document; or (ii) signed the document but is blind, illiterate and had to trust someone to tell them what they were signing;

or signed the document but has no understanding of the document without fault, due to defective education, illness or innate capacity. The defence requires proof that; (i) he was not negligent (reasonable precautions must be taken, including finding out the general effect of the document); and (ii) there is a fundamental difference between what he signed and what he thought he signed.

In the instant case, although the plaintiff testified that she is afflicted by a cataract which resulted a significant sight impairment that requires surgical correction, it was clear in court that she is not blind. The extent of her impairment therefore could not be determined by court. On account of her condition as it is known to her, the plaintiff took reasonable precaution in having her daughter P.W.2 Hadija Mirembe with her to help in filling the savings account opening application standard form. P.W.2 testified that she was reading to the plaintiff the content of the form while the plaintiff was telling her what information to write the blank spaces. In the circumstances, it is not plausible that the plaintiff did not seek to find out from P.W.2, the general effect and content of the document, before signing it. In any event, the document is not fundamentally different from what she intended to execute or sign. There is no evidence to show that during this process, the defendant was put on notice of any frailty, infirmity or feebleness on the part of the plaintiff, whether of mind or body. It also is not the plaintiff's case that her signature was obtained unfairly through misrepresentation, duress or undue influence on the part of the defendant, or that the text of the contract was so small that it was impossible for her to decipher its content. For all intents and purposes therefore, she is bound by her signature. Her contention though is that the bank ought to have explained its content and sought her informed consent, which it never did.

In advancing that contention, the plaintiff relies on *The Bank of Uganda Financial Consumer Protection Guidelines, 2011*. By those guidelines the banking sector has recognised the importance of free, prior and informed consent. Clause 1 (a) and (b) (i) of the guidelines requires all financial services providers regulated by the Bank of Uganda in respect of business they transact in Uganda, to act fairly and reasonably in all its dealings with a consumer of their services, and not to engage in unfair, deceptive or aggressive practices such as threatening, intimidating, being violent towards, abusing, or humiliating a consumer. Clause 6 (2) (a) (i) of the guidelines requires financial services providers to explain clearly in plain language the key features of the range of products and services that the consumer is interested in so as to enable the consumer to arrive at an informed

decision about those products and services, including any charges and fees which would be incurred, prior to a consumer choosing a product or service. It is the duty of the Bank of Uganda to monitor these Financial Consumer Protection Guidelines to ensure that all financial services providers are meeting their obligations, and achieving service standards.

It is ordinarily sufficient if the bank officer ensures that the customer understands the particular nature of the transaction to which he has agreed and comprehends its legal effect. The principle then is that where there is a breach of a Code of banking practice, which is the banking industry's customer charter on good banking service, a court will not necessarily set aside a legal instrument, such as a mortgage or guarantee, where it is clear on the facts that even if the Code had been complied with, it would have made no difference to the customer's decision to enter into the transaction by signing the documents (see *Williams v. Commonwealth Bank of Australia [2013] NSWSC 335*). Where there was no pressure applied by the bank in procuring the customer's signature, such as where the customer is given the opportunity to obtain independent legal advice but the customer maintains a firm view that he or she wants to execute the instrument, the customer understood nature and effect of the document, and the terms of the document are not unjust or unreasonable, the document will not be voided.

The law will investigate the manner in which the intention to enter into the transaction was secured: how the intention was produced. If the intention was produced by an unacceptable means, the law will not permit the transaction to stand. The means used is regarded as an exercise of improper or undue influence, and hence unacceptable, whenever the consent thus procured ought not fairly to be treated as the expression of a person's free will. It is impossible to be more precise or definitive. The circumstances in which one person acquires influence over another, and the manner in which influence may be exercised, vary too widely to permit of any more specific criterion. The courts can set aside a transaction where a party can prove that they were under a special disadvantage when the transaction was executed and that the other party has unconscientiously taken advantage of it. This disadvantage must be substantial enough to seriously affect the ability of the innocent party to make a judgment as to his own best interests and it must be sufficiently evident to the other party.

There is no exhaustive list of disadvantages, but they may include poverty, or need of any kind, sickness, age, sex, infirmity of body of mind, drunkenness, illiteracy or lack of education, lack of assistance or explanation where assistance or explanation is necessary. Limited ability to speak, read, or write in English is also often considered in the question of special disadvantage, as is emotional dependency. Any level or combination of these and other factors can combine to lead to a finding of disadvantage. However, a single factor, such as age, is unlikely to lead to such a finding. There is no evidence in the instant case though to show that during the process of account opening, the defendant was put on notice of any frailty, infirmity or feebleness on the part of the plaintiff, whether of mind or body.

Once the elements of special disadvantage are made out, the other party must prove that the transaction was fair, just and reasonable, which will often be difficult to do in the absence of independent legal advice for the disadvantaged party, or evidence of the party's commercial acumen. The idea behind independent legal advice is to protect an individual from signing any document before understanding the risks of the transaction. In banker-customer relations, there are two requirements for establishing the (rebuttable) presumption of undue influence. First, there must be a relationship of influence. The second requirement is that the transaction must not be readily explicable on ordinary motives (see *Royal Bank of Scotland v. Etridge (AP) [2001] 3 WLR 1021; [2002] 2 AC 773*). If those two requirements are satisfied, so that there is a presumption of undue influence, the burden of proof shifts and it is for the party seeking to uphold the transaction to rebut the presumption by showing that the other party was not acting under undue influence (i.e. that the other party exercised free and independent judgment) when entering into the transaction.

Typically this occurs when one person places trust in another to look after his affairs and interests, and the latter betrays this trust by preferring his own interests. He abuses the influence he has acquired. It is not the plaintiff's case that the defendant exerted any undue influence over her at the time she signed the account opening forms. There is no evidence of overt acts of improper pressure or coercion such as unlawful threats. There is further no evidence to show that arising out of the relationship between the parties at the time of account opening, the defendant acquired over the plaintiff a measure of influence, or ascendancy, of which the defendant took unfair advantage. The relationship between them was not such that, without more, the plaintiff was disposed to agree

a course of action proposed by the defendant. The problem appears to be that the plaintiff at the time of that transaction was not conversant with digital banking, yet it was offered to her.

Automation and artificial intelligence, already an important part of consumer banking as more and more repetitive tasks become automated, delivers benefits not only for a bank's cost structure, but for its customers as well. Instead of having to travel to a branch office of the bank, customers can get instant, efficient automated customer service powered by advanced artificial intelligence. Customers can contact their bank any time through the internet, mobile, or email channels and receive quick, real-time decisions. Digitising money transfers, for instance, speeds the process and gives customers the flexibility and freedom to view their bank accounts and transact online or with their mobile app. The COVID-19 pandemic was an unprecedented catalyst for digital banking across the globe. With many branches temporarily shut down and most physical interactions minimised, retail bank consumers in Uganda had no choice but to embrace these self-service channels like never before. Mobile banking has made it convenient for customers to check account status, pay bills, transfer money, or withdraw cash from ATMs.

While digital banking has always symbolised convenience, it is not without risks of fraud. As digital channels have multiplied, so have the routes that fraudsters can use. With increased automation financial institutions have become some of the most targeted by fraudsters, due to their immediate access to funds and their ability to transfer them. Online businesses that require users to enter login or registration credentials have a responsibility to protect accounts. Financial institutions offering mobile banking are thus obliged to provide secure mechanisms for their customers to conduct their banking safely online. As such, banks have a duty to put in place robust fraud detection and prevention solutions to protect their assets, systems and customers. They have a duty to take reasonable measures to ensure that their digital banking systems and technology are secure and are regularly reviewed and updated for this purpose. Banks should know when a suspicious transaction or withdrawal takes place. They should ensure that transactions on their digital banking services can be traced and checked as long as they are received by their systems.

These duties come with corresponding obligations. For the security measures to be effective, the bank should provide the customer with regularly updated information on how to access digital

banking services, including details about their customer ID, selection of appropriate passwords and the availability of additional authentication or security options, how to maintain their security and what their liability for unauthorised transactions will be. Of critical importance is the online fraud vulnerabilities of many senior citizens who believe that mobile phones are for talking and not conducting banking transactions. Educating all age groups is important, but given the trusting nature of the seniors, specific focus on the warning signs and dangers lurking in digital banking would help this vulnerable group and potentially assist in preventing account takeovers.

Banks should inform the customer of the applicable terms and conditions relating to the use of digital banking services, including any fees and charges, and the current transaction limits that apply to digital banking services, which limits may change from time to time and are available upon request. The customers should be informed of the procedures they must follow to report unauthorised access to their confidential personal information, accounts or disputed transactions using digital banking services and be provided with effective and convenient means to notify the bank of security incidents and easily accessible contact points to report such activity as soon as they become aware of it.

It was the testimony of the defendant's Supervisor Digital Banking, D.W.1 Mr. Narisensio Turyatunga that the PIN to her account was sent to the plaintiff within 24 hours of opening of the account. The plaintiff must have activated the PIN since it is not possible to have the PIN activated after twenty four hours. No evidence was offered though as to whether or not the plaintiff was advised on how to access digital banking services and on how to maintain her security against unauthorised transactions on her account through the digital platform. However the defendant's Applications System Analyst, Multichannel, D.W.2 Mr. Ssebunya Andrew, testified that one of the security features put in place by the defendant is that the customer's mobile phone USSD Code used at the time of the account opening is pegged to the sim card, such that a customer can transact with only one phone which is registered. When performing any transaction, if the serial number of the phone and the one pegged to the account do not match, the account will be blocked. Reactivation is required if access is blocked. Some of the reasons for blocking an account are; failure to activate the single-use system-activated PIN within 24 hours, multiple unsuccessful

attempts to log in, and change of phone for app users. In the instant case, there was a reactivation of the account which occurred on 5th February, 2020.

On the flip side of digital banking duties, is the customers' responsibility to always keep their banking information, user IDs, passwords and PIN numbers confidential. Account takeovers happen when fraudsters acquire the login details of a legitimate user, and then use the account as their own. Therefore digital bank customers have a duty to prevent fraudsters from gaining access to their personal login details. Account takeover fraud often begins with compromised credentials that have been stolen or obtained through trickery. Because customers reuse and share their PINs, the risk of account takeover fraud grows exponentially. If a customer gives his or her online banking details to anyone, it comes with the risk of losing whatever protection the bank offers against unauthorised transactions. This could result in the customer being responsible for any unauthorised transactions on his or her account, and in such cases the customer will not be refunded for any resultant loss. The bank should therefore advise the customer to change their temporary password to a password of their choice known only to the customer since failure to change this temporary password immediately may be construed as negligence by the customer.

One of the interventions made available to the plaintiff in order to enhance the level of protection of her funds deposited on the account was her registration for sms notifications, so that she could receive alerts whenever there was a transaction on her account. The intention was that she would read the messages from the defendant bank that may pop up from time to time whenever there was a transaction on her account. Although D.W.2 Mr. Ssebunya Andrew testified that the sms log in respect of the plaintiff's number shows that she was sent an sms alert upon each transaction undertaken on her account whenever it occurred, she admitted having received only one such sms alert. However, the plaintiff testified that her daughter had access to the plaintiff's phone and it is her daughter who normally read the messages on the phone, for the plaintiff. In effect, the plaintiff compromised some of the security features put in place by the defendant for her protection and instead reposed her trust and confidence in her daughter. Unfortunately, the plaintiff could not tell whether or not her daughter transacted on her account using that phone. She as well could not tell whether or not money from her account was transmitted from her bank account to her mobile money account using that phone. She was not aware of any transaction of that nature.

It was the testimony of the plaintiff that since she opened the account, she has never lost her phone, nor given it to anyone, save her daughter P.W.2. It is always with her although her daughters are aware if her sight impairment. However by his investigations, the defendant's Applications System Analyst, Multichannel, D.W.2 Mr. Ssebunya Andrew, testified that he established that on 6th February, 2020 there was a transfer of funds from the plaintiff's account to a phone number that does not belong to the plaintiff. However, the transfer was initiated by the customer, or a person with access to the PIN of the customer. The PIN had been re-activated the previous day on 5th February, 2020. He came to the conclusion that "given the transactions on the plaintiff's account were carried out using her telephone number on her mobile phone, the only conclusion is that she was aware of the transactions." Upon examining the same transactions, the defendant's Supervisor of Digital Banking, D.W.1 Mr. Narisensio Turyatunga too came to the conclusion that the transactions were done with the authorisation of the plaintiff, based on the fact that "she received transaction alerts on her phone coupled with the fact that all transactions done on her phone or account could only be done with the knowledge of her PIN number which is only known by her." Their conclusions are backed by the sms Log to the plaintiff's mobile phone number 0773 710 077 and her corresponding MTN mobile money statement (exhibits D. Ex.1 and D. Ex.2 respectively).

Account takeover fraud is completed through a series of steps, typically starting with the use of compromised credentials. The fraudster begins by making small changes to an account, often changing the PIN so that the legitimate account owner can no longer access their own account. The fraudster then moves on to financial transactions, including money transfers, until the fraud is detected or the customer's account is drained. I find in the instant case that the defendant at the material time had in place a two-factor authentication buffer to prevent unauthorised activity and access to the plaintiff's bank account while using of the "CenteMobile" digital platform. The plaintiff's mobile phone USSD Code was pegged to her sim card for number 0773 710 077, such that she could transact with only one phone and its corresponding sim card which was registered by the bank. Any hacker had to be in possession of the plaintiff's two-factor authentication; the actual phone and its corresponding sim card. Both authentication buffers were under the personal custody and control of the plaintiff at all material time, and not the defendant. All the impugned transactions were executed using that phone and its corresponding sim card.

The risk of loss for an unauthorised transaction lies with a customer if the bank can establish that the security procedure it has in place is a commercially reasonable method of providing security against unauthorised payment orders. In her own admission, at all material time the plaintiff never lost her phone, nor gave it to anyone, save her daughter P.W.2. Fraudsters rarely possess multiple types of authentication, so access to accounts is denied when they attempt unauthorised access. They can only do so after accessing PINs, answers to security questions and other personal information related to the customer, which information was exclusively known by the plaintiff. Although the account takeover sequence can be initiated through various means, fraudsters may use social interaction to prompt individuals into divulging account information. This appears to me to be the most probable explanation of the events in this case. In the circumstances the conclusion that these transactions were either undertaken by her, with her authorisation or due to her negligence, is inescapable. Whichever the fact may be, the defendant cannot be held responsible.

3rd issue; what are the remedies available to the parties.

Digital banking platforms fraud most commonly results from the compromise of an account. The fraudster tricks the account holder into providing their PIN for the account. Once compromised, the fraudster will use the account to transfer money to a different account and abscond with the money. The fraud leaves the two parties with a claim against each other, the bank has paid out the money, but the payment went to the fraudster; while the account holder has not received a payment. The question becomes, who is responsible for the loss?

Under the "imposter rule" which shifts the risk of loss from depositor or drawee banks to the drawer of checks, the party who was in the best position to prevent a forgery by exercising reasonable care suffers the loss. The principle behind the imposter rule is that the drawer of the check is in a better position to detect a fraud by one of its agents or employees than the drawee or depositor bank. Losses attributable to fraud should be borne by the parties in the best position to prevent the fraud (see *Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc., 759 F. App'x 348 at 357*). Similarly in cases of digital banking frauds, the party with better opportunity and in the better position to discover the fraudulent behaviour, or in the best position to prevent it, bears

the responsibility for the loss (see *Arrow Truck Sales Inc. v. Top Quality Truck & Equipment Inc. Case No. 8:14-cv-2052-T-30TGW*). In the instant case, with the two-factor authentication buffer put in place by the defendant to prevent online digital fraud on its "CenteMobile" service, the controls were squarely and unilaterally in the hands of the plaintiff.

There is no set standard to determine who was in the best position to prevent a loss. On the facts of this case though, the plaintiff was in the best position to prevent any fraud on her account and should accordingly bear any loss incurred as a result of compromising that system. The imposter rule does not protect banks from claims of commercial bad faith, i.e. knowing participation in a fraudulent scheme, wary vigilance or even suspicious circumstances which might well have induced a prudent banker to investigate. I however have not found any situation created by the defendant in the management of its two-factor authentication buffer that allowed third-party fraudsters to interfere with and compromise the plaintiff's bank account, yet the plaintiff was in a better position to avoid the loss. Therefore in conclusion, the suit fails and it is dismissed with costs to the defendant.

Delivered electronically this 18th day of July, 2022

……Stephen Mubiru……..
Stephen Mubiru
Judge,
18th July, 2022.