BANK CUSTOMERS COULD BE HELD LIABLE FOR BANKING FRAUD LOSSES

Account-holders may be held liable for loss suffered due to banking fraud

On 18 July 2022, the Ugandan High Court issued a landmark decision on the liability for loss suffered due to digital bank fraud in the case of ***Aida Atiku versus Centenary Rural Development Bank Limited, (the defendant/bank) Civil Suit No. 0754 of 2020.***

The case concerned an account holder with Centenary Bank who lost a substantial amount of the money that she had deposited in her account due to unauthorised transactions. The court was put to task to apportion liability for the loss suffered due to the unauthorised transactions. The court ruled that the party who is best placed to prevent a fraudulent activity will bear the loss. In this case, the court found that the loss lay with the account holder as the account holder had negligently allowed a third party to access her bank account leading to the fraudulent transactions. In addition, the court ruled that Centenary Bank would not be held liable as the Bank had put in place commercially reasonable security features which the account holder had jeopardised.

Factual Background

Aida Atiku (the **plaintiff**) opened a personal savings bank account with Centenary Bank (the **defendant**) at a branch along Namirembe Road in Kampala on 2 January 2020. The plaintiff deposited Ugandan Shillings (USH) 56,320,000 into the account between the period of 4 to 10 January 2020. Notably, the plaintiff was accompanied by her then 42-year-old daughter as she had a sight impairment and could not read the account opening documentation. Her daughter read out the contents of the account opening forms and filled the forms in line with the plaintiff's instructions.

In January 2020, the plaintiff made a withdrawal of USH 700,000. Upon returning to the bank in August in the same year to withdraw the remaining amount of USH 55.6 million, the plaintiff was shocked to find that the account balance had been depleted. The defendant's

staff informed her that withdrawals had been made over time using the CenteMobile platform, a digital banking platform that allows the defendant's customers to transact remotely using their mobile devices. The plaintiff maintained that she had only made a withdrawal of USH 700,000 and the USH 55.6 million had been fraudulently withdrawn from her account.

Consequently, the three main issues for determination before the High Court of Uganda were:

1. whether or not the plaintiff's account was fraudulently and / or negligently debited by the Bank;
2. whether or not the Bank is liable for the fraudulent and / or negligent withdrawals made on the plaintiff's account; and
3. what remedies are available to the parties.

Analysis

The High Court in arriving at its decision considered several issues such as the bank-customer relationship, principles of contract formation and liability for digital bank fraud.

Account opening formalities and the question of misrepresentation and undue influence

The court first addressed the issue of whether the plaintiff had applied for the digital banking service. In doing so, the court reiterated the common law duty on the signatory of a contract to make sure they understand the terms and conditions before signing. The effect of this duty is that a signature acts as conclusive evidence that the signatory has read, understood, and consents to the terms and conditions set out in the contract. The binding nature of the signature is only vitiated where the signature was obtained unfairly through misrepresentation, duress, or undue influence, or where the text of a contract is so small that it is impossible to decipher.

In this case, the court found that the plaintiff had signed the standard account opening forms including a standard form containing a clause approving the registration to the digital banking service. The plaintiff testified that she was afflicted by a cataract which caused a significant eye impairment. Due to her condition, she had been accompanied by her daughter to the bank and it was her daughter who had read all the contents of the forms to her. Against this background, the plaintiff's contention was that the Bank ought to have explained the contents of the forms and sought her informed consent, which it never did.

The court concluded that her signature bound her to the contents of the contract since none of the vitiating factors applied and she had therefore been legitimately registered to the digital services. Court stated that it could 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 had unconscientiously taken advantage of it. The disadvantage must however 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. , In this case the court found that the plaintiff did not adduce any evidence to show that during the process of account opening the defendant was put on any notice of frailty or infirmity of her body or mind. The court further found that there was no evidence of undue influence or coercion and the problem was simply that the plaintiff was not conversant with digital banking at the time of the

transaction and yet the Bank offered the service to her.

Bank's obligation to a customer and the associated risk of fraud in digital banking

The court proceeded to set out the obligations of financial institutions to provide secure mechanisms for their customers to conduct their banking activities safely in light of the growth of digital banking and associated risks of digital fraud. Specifically, the court stated that banks have a duty to put in place robust fraud detection and prevention solutions to protect their assets, systems, and customers. The scope of this duty includes taking commercially reasonable measures to ensure that the digital banking systems are secure.

The court considered the security mechanisms provided to account holders by the defendant through a witness statement of the defendant's Applications System Analyst. The witness expounded on a two-step authentication buffer whereby the customer's mobile phone USSD Code, used at the time of the account opening, is pegged to their sim card, such that a customer can transact with only one phone which is registered and its corresponding sim card. 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. Further, the defendant informed the Court that the plaintiff had registered for the SMS notifications to be sent to her after each transaction, and that she was in fact sent an SMS alert upon each transaction undertaken on her account whenever it occurred.

The plaintiff testified that she had not lost her phone since opening her account. However, she testified that her daughter had access to the phone and her security credentials, and that it was her daughter who normally read to her the messages on the phone. She also contended that she had only received one SMS notification of a transaction since opening her account.

The thrust of the defendant's defence was that the plaintiff was aware of the transactions given that any digital banking transaction required both the plaintiff's registered mobile phone and the corresponding mobile phone number and her PIN number, which was only known by her.

Customer's obligation to prevent third party access

The court found that the plaintiff had 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. Court went on to state that while banks have an obligation to put in place secure systems, account holders have corresponding responsibilities to ensure they keep their banking information and security credentials secure and confidential. Failure to do so would effectively obliterate any protection that the bank offers against unauthorised transactions.

Court's finding

After the review of the evidence, the court was satisfied that the two-factor authentication buffer put in place by the defendant was sufficient to prevent any unauthorised activities and access to the plaintiff's bank account while using the digital banking platform. The court found that both authentication buffers were under the personal custody and control of the plaintiff at all material times, and not the defendant. Additionally, all the impugned transactions had been executed using the plaintiff's phone and its corresponding sim card. the court concluded that the transactions on the

plaintiff's account had either been undertaken by her, with her authorisation or due to her negligence, and the defendant could therefore not be held responsible.

In determining who was responsible to bear the loss of the fraud, the court relied on the imposter rule which dictates that losses attributable to fraud should be borne by the parties in the best position to prevent the fraud. The court noted that although there was no set standard to determine which party was best placed to prevent fraud, in this particular case, the court was certain that based on the set of facts available, the plaintiff was best placed to prevent the fraud.

The court also noted that fraudsters may use various channels to gain access to a bank customer's account including the use of social interaction to prompt the customer to divulge information which should otherwise not be shared with third parties.

Conclusion

There has been a proliferation of bank fraud cases especially with the increased use of digital banking. While banks have put in place security systems to protect unauthorised transactions, bank customers have found themselves victims of fraud.

The decision of the High Court of Uganda is of interest to both banks and bank customers. The decision is a victory for banks as the banks are now assured of limited liability in cases of fraud where they can prove that they have put in place proper systems to prevent unauthorised access to a bank account.

Bank customers will now be required to ensure that they take reasonable steps to ensure that they do not negligently allow third parties to access their bank accounts. Failure to prevent such unauthorised access, bank customers will be liable for any loss they suffer.

The case however highlights the particular care that banks should take in relation to customers with disabilities of body or mind and confirms that extra precautions are needed where it is reasonable to assume that the disadvantaged customers may need the assistance of others in order to authorise transactions. This case also highlights banks' corresponding obligations to ensure that the security measures put in place are effective by; providing customers with regularly updated information on how to access digital banking services, with special concern being given to senior citizens; advising customers on selection of appropriate passwords; the availability of additional authentication or security options; informing customers about the applicable terms and conditions relating to the use of digital banking services; and lastly informing customers about the procedures they must follow to report unauthorised access to their confidential personal information, account and disputed transactions using digital banking services.

Sonal Sejpal
Partner
ALN Kenya | Anjarwalla & Khanna
sonal.sejpal@aln.africa

Fiona Magona
Partner
ALN Uganda | MMAKS Advocates
magona@ug.africalegalnetwork.com

ALGERIA | CÔTE D'IVOIRE | ETHIOPIA | GUINEA | KENYA | MADAGASCAR | MALAWI | MAURITIUS | MOROCCO | NIGERIA | RWANDA | SUDAN | TANZANIA | UGANDA | ZAMBIA • UAE