When is a bank liable for unauthorised digital withdrawals?

Lessons from Nakku Joweria v Stanbic Bank (U) Limited

CASE
Nakku Joweria v Stanbic Bank (U) Limited
Civil Suit No. 197 of 2024, [2026] UGCommC 368

DECISION DATE
3 August 2026
Commercial Court of Uganda

OUTCOME
Bank found not liable
Credentials compromised; no breach of duty by bank

In a decision handed down on 3 August 2026, the Commercial Division of the High Court of Uganda revisited the question: when a customer's credentials are compromised and money disappears from their account, who bears the loss?

Background of the dispute

The plaintiff's claim:

The plaintiff instituted the suit against the defendant, alleging a breach of duty arising from the unauthorised withdrawal of UGX 68,000,000 from her account. She sought recovery of the withdrawn funds, together with interest, general damages, and costs of the suit. The plaintiff averred that she had maintained a savings account with the defendant bank since 2001, from which UGX 68,000,000 was unlawfully withdrawn between 7th and 8th February 2023 through 17 unauthorised transactions conducted via the bank's Flexipay platform using four unknown Airtel numbers. She contended that the transactions occurred within 24 hours without detection by the defendant bank and that she had neither authorised nor sanctioned them. As a result, she alleged that the defendant breached its duty and caused her financial loss, inconvenience, and emotional distress. The defendant offered to settle the claim by refunding half of the lost amount, but the plaintiff rejected the offer as inadequate and unfair.

The bank's defence:

The defendant denied liability, contending that the plaintiff had lost her phone and KYC credentials on 6th February 2023, which were subsequently used to register her for the Flexipay service and conduct the unauthorised withdrawals. The defendant argued that the plaintiff only reported the loss on 6th March 2023, after UGX 68,000,000 had already been withdrawn on 7th and 8th February 2023, and that she had failed to promptly notify the bank as required under the account terms. It further maintained that the transactions were initiated through the plaintiff's Flexipay-linked wallet number 0782585291 and thus there was no breach of duty. The parties unsuccessfully negotiated a settlement of UGX 34,000,000, which the defendant stated was not an admission of liability.

The plaintiff's reply:

In response to the defense, the plaintiff maintained that she had promptly reported the loss of her phone to Airtel Uganda and MTN Uganda on the same day and argued that the transactions should have alerted the bank, particularly because her savings account had been dormant for about five years. She further denied losing her National ID or enrolling for Flexipay, stating that the account did not require the service.

Issues:

1. Whether the bank owed the plaintiff, as its customer, a duty of care.
2. Whether the bank was liable for the unauthorised withdrawals from her account.
3. What remedies, if any, were available to the parties.

Court Holding:

The court addressed the first two issues together, holding that a bank owes every customer a duty to exercise reasonable skill and care in operating and safeguarding their account. The real question, the court said, was whether that duty had actually been breached on the facts.

A central finding was that the plaintiff's banking credentials had, in fact, been compromised after she lost her phone. Because Flexipay could be registered remotely by USSD or through the app without any need to visit a branch. This means that whoever held her phone and National ID was able to enrol her for the service on 7 February 2023 and then carry out the withdrawals that followed. The court was firm that this responsibility cuts both ways: customers, too, must safeguard their credentials, and where a phone or registered SIM is lost, they must notify the bank promptly, not only the telecom operator or the police.

> *"It is prudent for a customer of a bank who has lost his or her phone or the account-registered SIM card/number to report the said loss to the bank as soon as possible, because the loss of the said phone and SIM card renders the bank account susceptible to fraud by third parties, and it is not enough for a customer to report the said loss to the police only."*
>
> *– Equity Bank (U) Ltd v Bamwite Augustine Muhindo, Civil Appeal No. 59 of 2025*

On the bank's own obligations, the court reaffirmed that financial institutions offering mobile banking carry a genuine duty to build and maintain robust fraud-detection and security systems for their digital channels.

> *"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."*
>
> *– Aida Atiku v Centenary Rural Development Bank Limited*

Even so, the court declined to find that Stanbic should have automatically flagged the transactions simply because they were unusual. Despite several failed attempts to enrol the account and withdraw funds before the successful transactions went through, the evidence showed that the bank's own authentication procedures had been properly followed throughout i.e validation and authentication codes were sent to the plaintiff's registered number, and the Flexipay transactions were completed using credentials genuinely tied to her account.

> *"A bank's duty to take additional care in preventing fraud is triggered only where there are specific and reasonable indicators giving rise to a genuine suspicion of fraud. An unusual or abnormal transaction, by itself, is insufficient; mere concern or discomfort about a transaction does not impose a heightened duty on the bank."*
>
> — *Barclays Bank of Uganda Limited v Eron Kabachwamba, Civil Appeal No. 10 of 2015*

Finding no evidence that Stanbic had departed from its required authentication or fraud-prevention procedures, the court held that the bank could not be made liable simply because the plaintiff's credentials had, through no fault of the bank, fallen into the wrong hands.

The Court's conclusion:

The court concluded that while a bank owes its customers a duty to exercise reasonable skill and care in safeguarding accounts and processing transactions, that duty is not absolute. Where a customer's authentication credentials have been compromised and no breach of the bank's own duty is established, liability cannot be imposed on the bank merely because unauthorised transactions occurred. Stanbic Bank was accordingly held not liable for the disputed withdrawals.

Key takeaways for banks and customers:

- *Banks' duty of care:* Banks must exercise reasonable skill and care in safeguarding customer accounts, processing transactions, and maintaining secure digital banking systems.

- *No automatic liability for unauthorised transactions*. The customer must establish that the bank breached its duty of care; the mere fact that money was withdrawn fraudulently is insufficient.

- *Customers' duty to protect banking credentials.* Customers have a duty to safeguard their phones, SIM cards, PINs, passwords and other authentication details, and must immediately notify the bank when these are lost or compromised.

- *Unusual transactions alone do not trigger heightened liability. A* transaction must present specific and reasonable indicators of fraud before a bank is expected to take additional protective measures. Mere unusual activity is not enough. Banks have a duty to obey its customer's mandate and it may be liable to a customer if it fails to comply with a payment instruction.

- *Liability depends on the conduct of both parties.* Where customer credentials are compromised, the court may consider the steps taken by the customer to protect and report the compromised credentials, as well as whether the bank implemented and followed reasonable authentication, security, and fraud-prevention procedures.

A practical note:

For banks and fintechs, this decision is a reminder that well-documented, consistently applied authentication procedures remain the strongest defence against liability claims of this kind. For customers, it is an equally important reminder that in a mobile-first banking environment, a lost phone or SIM card is not a minor inconvenience, it is a live security risk that must be reported to the bank without delay. As digital and mobile financial services continue to expand across Uganda and the wider East African region, cases like this one will increasingly shape how courts allocate risk between financial institutions and the customers who trust them with their money.

ABOUT THE AUTHOR

Salwa Mukoda Okiring, Esq.

C.E.O, Infocite Consulting | *Law Lecturer, Victoria University School of Law* | *Host-Real Talk with Salwa Podcast*

Salwa writes on banking, commercial and investment law across Uganda and East Africa through Infocite. Visit **www.infociteconsulting.com** to learn more.