CM ADVOCATES LLP

THE 16-MINUTE FRAUD DILEMMA;
Who Bears the Risk When Digital Banking Goes Wrong?

From the temples of ancient Mesopotamia, the money lenders of ancient Greece to the touch of a screen on your phone in a mobile banking app, the world of banking has experienced a revolution like no other. With these advancements, certain risks have evolved; like what happens when a stranger having access to your credentials and exploiting system vulnerabilities, initiates transactions on a customer's account? This was the question the court in ***Milimani SCCCOMM E6743 James Njoroge vs. Stanbic Bank Kenya Limited*** had to grapple with, where a system's vulnerabilities are exploited to a customer's detriment, who bears the risk of such vulnerabilities?

FACTS

The Claimant who had been operating a traditional bank account with the Respondent for 10 years, sued his bank for Kshs. 851,000 and for general damages for breach of the duty of care. Following a robbery on 13th July 2025 at 6:30 am where the Claimant got drugged and incapacitated losing his national identity card, ATM cards and his mobile phone linked to his bank account; a digital banking profile was created linked to his account at 2:48 pm that day. Subsequently between 3:09 pm to 3:25 pm, 3 transactions totalling to Kshs. 1,001,000 were processed. His wife then notified his bank at 5:19 pm and the account was then restricted at 5:59 pm. The bank then recovered a sum of Kshs. 490,000 from the receiving account. The Claimant sought to recover the outstanding balance of Kshs. 511,000.

The bank in its defence, argued that the banker-customer relationship was a reciprocal one, where the customer bears a significant responsibility to safeguard their

own access credentials. The bank contended that they acted with all due diligence because the transactions were initiated through the Claimant's registered mobile number and verified using his specific, private details (his National ID, date of birth, and three separate One-Time Passwords (OTPs)). From the bank's perspective, since the "right keys" were used to unlock the account, they had no objective reason to suspect the instructions were fraudulent.

It also emphasized the 11-hour gap between the 6:30 am robbery and the 5:19 pm report, arguing that this delay was the material cause of the loss. Furthermore, that under their standard terms and conditions, the Claimant had a contractual duty to protect his PIN and mobile device; by failing to do so, they argued he had breached his own duty of care.

Finally, the bank clarified that their successful recovery of a portion of the funds was a standard mitigation effort and not an admission of negligence as it was initiated after notice was received, while also challenging the total quantum of the claim by noting that some funds were transferred to the Claimant's own M-Pesa account.

WHAT WAS THE COURT'S FINDING?

The Court identified three issues for determination:

a. Whether the bank breached its duty of care and fiduciary obligations to the claimant?
b. Whether the claimant breached his duty to safeguard his bank credentials?
c. Whether the claimant was entitled to the reliefs sought and the quantum of the claim?

On the first issue, the court held that the bank did owe a duty of care to the Claimant and had breached this duty. The bank had failed to maintain a secure gate keeping system but instead relied on a self registration process that was vulnerable to fraud thus failing to protect a long-standing customer from a foreseeable risk. As the custodian of the digital banking platform, it was obligated to be a vigilant guardian and put in place measures to reasonably prevent fraud. The peculiarity of the case was that the account was entirely offline for 10 years until the digital profile was activated and the subsequent transactions initiated. The Court noted that the bank had a duty as the "gate keeper" of its clients' monies to prevent the occurrence of the fraud placing reliance on the decision in ***Family Bank Limited v Kiarie [2026] KEHC 9414 (KLR)*** to that effect. The bank's onboarding process for its digital platform was found to be vulnerable. Relying on information provided by the Claimant 10 years ago at the point of registering his physical account failed to meet the verification standards for a digital account.

Further, the bank's failure to flag the subsequent transactions amounting to Kshs. 1,001,000 made within 16 minutes on a newly created digital profile was considered a systemic failure. In this regard, the court relied on the decision in ***Diamond Trust Bank Kenya Ltd v Kariuki & another [2026] KEHC 9771 (KLR)*** that a bank is mandated to flag suspicious transactions especially in the circumstances where large transactions were made on a new digital profile of a previously dormant account.

The bank's recovery of Kshs. 490,000 after it was notified by the Claimant, was treated as a recognition by the bank that the transactions were largely suspect and that it had a responsibility to attempt recovery as was held in ***Co-operative Bank of Kenya Ltd v Mutuku [2025] KEHC 4324 (KLR)***. Subsequently, even where the third party

receiving the funds is identifiable, the court held that the primary responsibility to restore the customer's funds fell upon the bank.

On the second issue, the court having noted that the loss was primarily caused by vulnerabilities in the bank's system and a failure to flag the transactions in the circumstances, found that the Claimant had not breached his customer obligation by giving his details to the wrong party, additionally, he had notified the bank of the fraudulent transactions.

Lastly, on whether the Claimant was entitled to his claim for 851,000, the court awarded the claimant the sum of Kshs. 511,000 being the difference between the sums lost less the recovered sums. The court declined to make an award for general damages as the claim arose from a breach of contract whose loss was quantifiable.

WHAT DOES THIS DECISION MEAN FOR BANKS AND CUSTOMERS?

Who Absorbs the Risk? From the decision the "risk of the system" is borne by the service provider; when a bank creates a digital channel, it assumes a fiduciary duty to ensure that channel is robust.

The risk is absorbed by the bank in three specific scenarios:

1. **Structural Vulnerability:** If the registration process relies on static data (like ID numbers and dates of birth) which are easily stolen, the bank is liable for the inherent insecurity of its own design.
2. **Algorithmic Failure:** Banks are expected to have intelligent fraud detection. A sudden burst of high-value activity on a historically dormant or offline account is a red flag that the bank ignores at its own peril.
3. **The "Right Key" Fallacy:** Even if a thief uses the "right key" (a stolen phone or PIN), the bank is liable if it failed to verify that the person holding the key was the actual customer through secondary means.

What Banks Can Do to Mitigate Risk To avoid the systemic negligence trap, financial institutions must move beyond the closed-loop SMS OTP system. Several areas for reform are:

- **Enhanced (Know Your Customer) KYC for Digital On-boarding:** For customers who have been "offline" for years, self-registration for digital banking should require more than just an OTP. Banks should implement biometric matching.
- **Transaction Velocity Limits:** Automated kill-switches should be triggered when a new digital profile is created. A 24-hour "cooling-off" period with low transaction limits for new profiles would have prevented the loss in Njoroge vs. Stanbic Bank.
- **Behavioural Analytics:** Banks must deploy systems that recognize deviations from a customer's historical baseline. A 10-year offline customer suddenly transferring a million shillings in 16 minutes on a newly created digital profile is a textbook anomaly that should require human intervention before approval.
- **Restitutionary Proactivity:** As noted in the judgment, when a bank identifies the recipient of fraudulent funds, it has a duty to pursue those funds immediately for the benefit of its customer and its own indemnification.

CONCLUSION

The key takeaway from the decision is that the banker-customer contract is no longer just

about keeping money safe in a vault; it is about keeping data safe in a network. If the network is the vulnerability, the bank, not the customer, will pay the price.

This publication is intended for general information purposes only and does not constitute legal advice or a legal opinion. It is not intended to be a substitute for legal advice on any specific matter. The application of the law will depend on the particular facts and circumstances of each case. If you require advice specific to your circumstances, please contact us via mombasaoffice@cmadvocates.com or your usual contact at our firm.

Contact our Practice Unit

Dispute Resolution & Appellate Practice Group
E: disputeresolution@cmadvocates.com

Contributors:

David Muthukia
Associate Advocate
dmuthukia@cmadvocates.com

CM Advocates LLP – Contact Details

Head Office Nairobi
I&M Bank House, 7th Floor, 2nd Ngong Avenue
T: +254 20 2210978 or +254 716 209673
P.O. Box 22588 – 00505, Nairobi Kenya
E: law@cmadvocates.com

Mombasa Office
Links Plaza, 3rd Floor, Links Road, Nyali
T: +254 041 447 0758 / +254 41 447 0548
P.O. Box 90056 – 80100, Mombasa Kenya
E: mombasaoffice@cmadvocates.com

Regional Presence
Uganda | Tanzania | Rwanda | Zambia | Ethiopia | South Sudan

www.cmadvocates.com

Disclaimer: *This publication is for informational purposes only and does not constitute legal advice. For tailored legal support, please consult our team.*

© CM Advocates LLP, 2026