



REPUBLIC OF KENYA



KENYA LAW
THE NATIONAL COUNCIL FOR LAW REPORTING
Where Legal Information is Public Knowledge

**Kabaru v Craft Silicon Limited (Cause 83 of 2019)
[2023] KEELRC 1584 (KLR) (30 June 2023) (Judgment)**

Neutral citation: [2023] KEELRC 1584 (KLR)

**REPUBLIC OF KENYA
IN THE EMPLOYMENT AND LABOUR RELATIONS COURT AT NAIROBI
CAUSE 83 OF 2019**

**J RIKA, J
JUNE 30, 2023**

BETWEEN

GIDEON MWANGI KABARU CLAIMANT

AND

CRAFT SILICON LIMITED RESPONDENT

JUDGMENT

1. The Claimant filed his Statement of Claim on February 11, 2019.
2. He states that he was employed by the Respondent on February 22, 2016, as a Software Developer. His contract was for a period of 2 years. He was earning a monthly gross salary of Kshs 220,000. His contract was renewed for another 2 years, from February 22, 2018. His monthly gross salary was improved to Kshs 253,000.
3. He did not serve to the end of his contract. On July 30, 2018, the Respondent terminated his contract, alleging that the Claimant was involved in fraud.
4. He states that termination was unfair, contrary to the *Employment Act*, the Employee Handbook, and the *Constitution* of Kenya. The Respondent did not avail to him an important document for purposes of answering to the allegations against him - the Computer Forensic Investigation Report. The Report exculpated him.
5. The Management Officers who oversaw the termination process, did not have valid practicing certificates to act as Human Resource Management Professionals, under the *Human Resource Management Professionals Act*, 2012. The Respondent did not have at the time, any Human Resource Management Professional.
6. The Investigator found that the Claimant's login credentials were compromised, occasioning the alleged fraud. The Claimant was a victim of the fraud, rather than its architect.



7. He prays for Judgment against the Respondent for: -
 - a. Declaration that termination was unfair and unlawful.
 - b. 12 months' salary at Kshs 3,036,000 in compensation for unfair and unlawful termination.
 - c. 1-month salary in lieu of notice at Kshs 253,000.
 - d. Interest.
 - e. Certificate of Service to issue.
 - f. Costs.
 - g. Any other suitable order.
8. The Respondent filed its Statement of Response, on April 2, 2019. It is admitted that the Claimant was employed by the Respondent. On June 21, 2018, the Respondent received a call from Safaricom PLC, that there was security breach of the Respondent's system, resulting in suspicious m-pesa transactions.
9. Similar concerns were raised by Jamii Bora Bank, Standard Chartered Bank, Kenya Women Finance Trust, and Credit Bank, who all reported that there were suspicious activities in the Respondent's mobile banking platform. The Banks alerted the Respondent to investigate immediately.
10. Preliminary Investigations revealed that there were fraudulent transactions initiated internally by the Respondent's Staff; the Claimant and other colleagues logged into the Respondent's m-pesa server, and installed an application known as Key Logger, under the Java Application, so as to get the passwords of the Users, who were authorized to access m-pesa server; and the Key Logger was installed with the User 'Gideon Kabaru' the Claimant herein.
11. The Claimant and his colleagues, using the passwords obtained through the Java Application, logged into the m-pesa server, and sent requests to Safaricom PLC, to fraudulently credit various m-pesa mobile accounts, amounts totalling Kshs 91,176,192. The Claimant was directly, or indirectly involved in this fraud.
12. The fraud was reported to the DCI, who upon detailed investigations, established that the Claimant was directly involved. The ODPP preferred charges against the Claimant. He was arraigned before the Kiambu Chief Magistrate's Court, and charged with stealing Kshs. 91,176,192.
13. External Investigator hired by the Respondent concluded that there was malicious software introduced to the Respondent's system. It was introduced by the Claimant.
14. The Respondent held a meeting with the Claimant on July 30, 2018, and explained to him that the Respondent could not retain him. He was summarily dismissed. Termination process was overseen by Catherine Tole, a certified and registered member of the Institute of Human Resource Management. The Claimant was offered terminal dues, amounting to Kshs 64,431.
15. The Claimant filed a Reply to the Respondent's Statement of Response, on April 10, 2019. He reiterates his asseverations, and denies allegations of fraud, pleaded by the Respondent.
16. He was heard and closed his case, on February 7, 2023. The Respondent did not adduce evidence, and relies on the record. The matter was last mentioned on April 18, 2023, when the Parties confirmed filing and exchange of their closing submissions.
17. The Claimant adopted the contents of his Pleadings as summarized above, his witness statement and documents [1-9] on record.



18. Cross-examined, he stated that he was software and database developer. His role required high standards of honesty and mutual trust. He created software applications. The Respondent offers financial solutions. The Claimant discharged his role through a computer. He had access rights. He had Username, Gideon.Kabaru. The Username was unique. No 2 persons shared the Username.
19. On June 21, 2018, m-pesa server was compromised. He came to learn about this through other staff. A malicious application was introduced into the Respondent's system. The Respondent lost Kshs 91,176,192. He was not involved. He was away in Rwanda, on June 19, 2018. He was not told about the attack when he returned. He was summoned by the DCI in July 2018, and his phone and laptop confiscated. He did not immediately tell the DCI that his credentials were interfered with. He told them this after he was taken to their offices. He was aware that there was some tampering with his laptop. He did not adduce evidence before the Court, to show that he reported tampering to his supervisor. He became aware of the Investigation Report in September 2018. The Report was produced at the criminal case. The Report concluded that the Claimant's credentials were compromised. His name was used. He was not interrogated by the DCI. He was only made to record a statement.
20. He was charged with a criminal case. Several counts were presented. The Respondent did not have reasonable suspicion that the Claimant was involved in the fraud. He declined terminal dues offered to him, because he was required to execute discharge.
21. Redirected, the Claimant told the Court that Username is unique. He had a password. Investigators said they were not able to identify the persons behind the fraud. He did not introduce the Key Logger. He was not given a hearing by the Respondent. He was not responsible for ICT security.
22. The issues are whether the Claimant's contract was terminated for valid reason[s] under Sections 43 and 45 of the Employment Act; whether procedure was fair in accordance with Sections 41 and 45 of the Employment Act; and whether the remedies sought are merited.

The Court Finds: -

23. The Claimant's employment history, and the terms and conditions of employment with the Respondent, are not disputed. It is not disputed that the Respondent terminated the Claimant's contract on July 30, 2018, on allegations of fraud.
24. Reason[s]. The Respondent's business, is to offer financial solutions. On June 21, 2018, its ICT security system was breached, where money was credited to Safaricom mobile accounts fraudulently. Alarm was raised by Safaricom PLC, and a host of Banks, associated with the Respondent. The Respondent lost Kshs. 91,176,192.
25. How this was carried out, is captured in the Final Computer Forensic Investigation dated July 23, 2018. On June 21, 2018, the Respondent's m-pesa system was manipulated to perpetuate fraud. The Investigator found that various malicious software in the form of keyloggers, credential harvesters, and connection scripts to external IPs, were installed in various machines. Usernames 'default,' 'Michael,' 'Josephine,' 'administrator,' and 'Gideon.Kabaru,' were identified as responsible for the introduction of malicious software. The User Gideon.Kabaru's, was identified to have been compromised through a keylogger.
26. The Investigator was however, not able to pinpoint the individual responsible for the fraud, because a local User named default, was created and used to introduce some of the malicious software used to facilitate fraud.



27. The Claimant alleges that he was away in Rwanda when fraud took place and that he was exonerated by the Investigator.
28. The Court does not think that the Claimant was exonerated. All that the Investigator stated was that he was not able to pinpoint the individual responsible for the fraud, because a local User named 'default,' was created and used to introduce some of the malware used to facilitate fraud.
29. There was, in the view of the Court, multiple malware attack on the Respondent's ICT system. The Investigator was not able to assign individual responsibility, because there were multiple Usernames used.
30. This in the respectful view of the Court, was not the same thing as finding that the Claimant was not involved.
31. He confirmed on cross-examination that he was a Software Developer and Database Administrator. He was quite knowledgeable on the Respondent's ICT infrastructure. He created Software Applications. He told the Court that his role was defined by honesty and trust. His Username was Gideon. Kabaru. He confirmed that a Username is unique. It is not shared by any other person. When fraud was detected, the Claimant did not volunteer information to the DCI, that his credentials were interfered with. He only told them this, after he was summoned to the DCI Office. He was aware even before he was summoned, that his credentials had been interfered with. He did not have evidence showing that he reported interference to his Supervisor.
32. While the Claimant may successfully point to the Investigation Report's inability to pinpoint the individual responsible for fraud, in his criminal case at Kiambu, the standard of proof of reason for termination, under Section 43 of the [Employment Act](#), is not proof beyond reasonable doubt.
33. The Employer is only required to show that the reason or reasons for termination of a contract are matters that the Employer at the time of termination of the contract, genuinely believed to exist, and which caused the Employer to terminate the services of the Employee.
34. The Court is persuaded that the Respondent met the evidential burden, under Section 43 of the [Employment Act](#). Termination was substantively fair and justifiable.
35. Procedure. The Respondent pleads at paragraph 18 of its Statement of Response, that it held a meeting with the Claimant on July 30, 2018, and explained to him that the company could not retain him due to the fraud perpetrated by him, and he was summarily dismissed.
36. There was no letter to show cause, issued upon the Claimant after Investigations. There were no charges presented against the Claimant, and there was no disciplinary hearing at all.
37. The Respondent's Employee Handbook, provides that a disciplinary enquiry shall be held in all cases that could lead to dismissal. The Employee must be notified in writing of the alleged offence, the date, time and venue of the disciplinary enquiry, giving him at least 24 hours to prepare. The Employee shall be allowed the facility of representation. The Employee is allowed to mitigate, at the close of the hearing. It then falls on the CEO, to communicate the Respondent's decision to the Employee. The meeting held on July 30 2018 was not a disciplinary enquiry, contemplated by the Respondent's Employee Handbook.
38. This internal procedure, which mirrors Sections 41 and 45 of the [Employment Act](#), was disregarded. The Claimant was just called to Office by the Respondent on July 30, 2018, and issued the letter of summary dismissal.



39. The Claimant's submission that the Officers who presided over the disciplinary process did not have current practice certificates, issued under the *Human Resource Management Professionals Act*, is a red herring, aimed at detracting from the grave employment offences, he was faced with. He did not present evidence from the Registration Committee under the Act, showing that the Officers he accuses of lacking current practicing certificate, who dealt with his matter, were not compliant. The Respondent told the Court that Catherine Tole oversaw the process, and is a registered Human Resource Management Professional, and held the requisite certificates. The Claimant was taking away attention from himself, by alluding to the practicing status of the Officers who dealt with his matter.
40. Procedure was however, unfair.
41. Remedies. The Claimant served on an initial contract of 2 years, running from February 22, 2016. The contract was renewed for another 2 years, running from February 22, 2018. He served for 5 months under the 2nd contract, termination date being July 30, 2018. In total, he served for 2 years and 5 months.
42. He was largely responsible for the circumstances leading to premature termination of his contract. His Username was among the gateways used by fraudsters, to attack the Respondent's ICT infrastructure, and defraud the Respondent a huge amount of money, in the sum of Kshs 91,176,192. He did not honour his duty of trust, honesty and confidence. Procedure however, was deficient, and the Claimant is entitled to compensation for unfair termination which the Court grants, at equivalent of 1-month gross salary at Kshs. 253,000.
43. There was a valid reason to justify summary dismissal, and notice is therefore not payable.
44. Certificate of Service to issue.
45. No order on the costs and interest.

In Sum, It Is Ordered:

- a. It is declared that termination was based on valid reason, but unfair procedure.
- b. The Respondent shall pay to the Claimant equivalent of 1-month salary in compensation for unfair termination at Kshs. 253,000.
- c. Certificate of Service to issue.
- d. No order on the costs and interest.

DATED, SIGNED AND RELEASED TO THE PARTIES ELECTRONICALLY, VIA E-MAIL, AT NAIROBI, UNDER PRACTICE DIRECTION NO. 6[2] OF THE ELECTRONIC CASE MANAGEMENT PRACTICE DIRECTIONS, 2020, THIS 30TH DAY OF JUNE, 2023.

JAMES RIKA
JUDGE

