



REPUBLIC OF KENYA



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

**Nkonge v Yetu Sacco Limited (Cause E010 of 2022)
[2023] KEELRC 2268 (KLR) (29 September 2023) (Judgment)**

Neutral citation: [2023] KEELRC 2268 (KLR)

**REPUBLIC OF KENYA
IN THE EMPLOYMENT AND LABOUR RELATIONS COURT AT NYERI
CAUSE E010 OF 2022
ON MAKAU, J
SEPTEMBER 29, 2023**

BETWEEN

GLAD MAGERIA NKONGE CLAIMANT

AND

YETU SACCO LIMITED RESPONDENT

JUDGMENT

1. The claimant was employed by the respondent as the Head of ICT in the Sacco Head Quarters at Nkubu from 1st October, 2020 to 23rd June, 2022 when he received a letter terminating his employment for negligent performance of his work. He then brought this suit alleging that the termination was unfair because there was no valid reason, and that it was not done in accordance with a fair procedure. Therefore he prayed for the following reliefs:-
 - a. A declaration be and is hereby issued that the termination of the Claimant's contract of employment was unlawfully, unfairly, wrongfully and unprocedurally.
 - b. Payment of June salary.
 - c. Compensation for the leave days.
 - d. Payment of leave allowance
 - e. Payment in lieu of notice of 60 days
 - f. Payment in lieu of gratuity (2) years
 - g. Compensation for unfair and illegal termination in the sum of Kshs.1,754,400/= being an equivalent of 12 months' salary.
 - h. Damages for illegal use of photo against the data protection Act an IP property rights.



- i. Damages for publication of said photo and notice in the dailies without proof of guilt
 - j. Damages for emotional and psychological torture and lack of employment.
 - k. The respondent to be compelled to issue the claimant a certificate of service.
 - l. Costs of the suit
 - m. Any other relief that this honourable court may deem fit.
2. The respondent filed response to the claim denying that the termination was unfair and averred that it was grounded on a valid reason and the claimant was invited to a disciplinary hearing but he declined. It averred that the claimant performed his work negligently and carelessly as the Head of ICT and exposed the Sacco to hackers. It averred that the claimant created an Admin account with super rights on the Sacco's DMS Server (Admin 1) which he shared with the Personnel of Informak, a Company contracted by the Sacco to implement a DMS (Document Management System). As a result, the account was used by attackers to create another malicious account which was used to carry out fraud leading to a loss of Kshs.7.4 million. It therefore prayed for the suit to be dismissed with costs.

Evidence

3. The claimant testified as CW1. He basically adopted his written statement as his evidence and produced a bundle of documents in the list dated 22nd December 2022 as exhibits. In brief his evidence was that he joined the respondent on 1st October, 2020 as the ICT Manager in the ICT Department. His appointment was confirmed on 20th May, 2021 and in the same year he earned a certificate for the Employee of the year award.
4. His duties and responsibilities as the Head of ICT included inception and implementing and enforcing the Sacco's ICT Policy and Controls; review and recommend changes, updates to the ICT Policy; ensuring that all the telecommunication links are stable at all times; Website development and maintenance; maintaining proper system security at all time; developing and reviewing system process among other duties. He always exceeded his targets leading to tremendous increase in revenue. He never had any disciplinary issues with Sacco.
5. On 14th May, 2022 he was in Kitengela with a team doing visibility study when he received a phone call around 5 or 6pm, from the Accountant alleging that he had paid for goods but received no transaction message. He was not supposed to access the servers while away from the office but due to the complaint raised after work, he checked the system and noticed messages hanging and the system intruded. He then contacted the system vendor of the SMS services and the error was corrected, and all the hanging SMSs were delivered.
6. On 15th May, 2022 he received another call at 6pm from the Sacco's Chief Cashier Mr.Samuel Mwirigi saying that a client had alleged that he received SMS indicating a withdrawal of funds. He then checked the system again and contacted the Mobile Services Vendor and the services were put off. He then swung into investigations to see which accounts were transacted that night. The fraud was happening through Mpesa and transfer to external banks and therefore he contacted Safaricom and the other banks to suspend the accounts so that the money is not withdrawn.
7. On Monday 16th May, 2022, he reported to work and discovered that there was user account (Admin 1) created on 14th May, 2022 at 11.22AM and it had been used to create other links for withdrawing money fraudulently. He suspended the user account and notified the Sacco CEO.



8. The attackers were remotely connected using a software which enabled them to work from outside Sacco. The software was installed in the system on 14th May 2022 at 11.33Am. He then prepared a report on attack and forwarded to the CEO who asked him to write letters to the banks to suspend the said accounts and the CEO signed them. He also made a report of the attack to the DCI.
9. On 17th May, 2022, two clients in the external banks called him about funds deposited in their accounts and he referred them to the CEO. He never got to know what happened thereafter.
10. He denied that he was the one who created DMS account called admin 1 that led to his dismissal. He admitted to having been invited to disciplinary hearing vide a letter dated 8th June, 2022 which he received on 11th June 2022. However, the notice was too short for him and the charge was not clear to him and therefore he wrote an email to the HR Manager requesting for rescheduling of the hearing and particulars of the charges.
11. No response was sent to him and the hearing proceeded in his absence on 14th June 2022 at Nkubu while he was in Nairobi. When he reported back from suspension on 24th June 2022, he was shocked to receive a termination letter dated 22nd June 2022 which asked him to clear with the Sacco.
12. He filed an appeal on 27th June, 2022 but then he saw a newspaper notice saying that he was no longer an employee of the Sacco. His appeal was never heard as he never received any word about it thereafter. In his view the Newspaper notice was in bad faith and discriminatory.
13. He cleared with the Sacco but he was not paid his terminal dues including leave allowance, salary for June 2022 and 41 leave days. He was also not given certificate of service. His salary was Kshs.75,800.00 as at the time of exit. He contended that his career was affected by the unfair termination of his employment.
14. On cross examination, he stated that he had been an IT Practitioner for 9 years. He admitted that he had privileged rights as the Head of ICT in the Sacco. He maintained that his junior Mr. Henry Mburugu had similar privileged rights as the Line Manager ICT and that why he could take charge while he was away.
15. He testified that Informak was contracted by the Sacco through a procurement committee and not through his sole recommendation. The committee picked Informak from a list of five Vendors after a background check by a team of five employees who were sent by the CEO to entities where the vendor had installed the system.
16. He testified that Informak was first to arrange the registry and deliver shelves, and secondly digitize the files in the shelves and then store them in Sacco servers. The registry department was involved in the first mandate which was done from November, 2021 and ended in February, 2022. He was however involved in the second phase of digitizing the files in the registry. All the ICT department and the HR department supported the vendor in doing its work.
17. He admitted that as the head of ICT, he could access the system remotely, that is, when he was away from the office. He could also change passwords. He admitted that he created a user account named DMS for Informak to facilitate them in doing their work. He opened the account after the vendor filled the required form and prompted the vendor to change the password and they changed. Thereafter the claimant could not know the new password.
18. He admitted that Informak had access to the server they were configuring and the computers allocated to them for the work. They also had access to the customers' names and account data from the physical files in the registry. He contended that the fraud was done remotely through DWs server. He discovered



that the software accessing the system remotely was connected to the DMS user but it was installed through admin 1 account. The admin 1 account was created on 14th May, 2022 but he did not know who created it because only Informak had the password to access the DMS account. He stated that Kshs.7.4 million was lost during the attack but he took the necessary remedial steps to stop the fraud. However, he was suspended before concluding the investigations.

19. He admitted that the respondent's HR Manual clause 2.4(b) provided for termination of employment for gross misconduct and without notice or salary in lieu of notice. He stated that he was doing personal work in Nairobi while on compulsory leave and then he fell sick. He denied that his Branch Manager Mr. Elkana Ronio had approached him to do something for a common good.
20. On re-examination he contended that it was necessary to create the DMS account for Informak since without it they could not upload any data to the server. He reiterated that he was sent on compulsory leave before investigating the root of the fraud. Finally, he contended that publishing his photo in the newspaper was malicious.
21. Serah Kibiti, respondent's internal auditor testified as RW1. She adopted her written statement and produced 5 documents as exhibits. In brief she stated that the claimant's duties as the Head of ICT included ensuring system integrity, availability and security at all times. She testified that the claimant had the Admin user rights meaning that he controls the system and could give or deny rights to the staff. He also had remote access rights.
22. She further stated that the Sacco lost Kshs.7,311,499 through online fraud and when the claimant was invited for a disciplinary hearing he failed to attend without any reason and he was dismissed.
23. On cross-examination, she stated that only the claimant could create Admin 1 account since all the users in the system were created by him. She contended that the claimant created DMS account for Informak during the implementation of the system. She accused the claimant of committing the fraud or in the alternative negligent performance of duty that caused the fraud. However, she admitted that she is not an ICT Professional but finance expert.
24. She confirmed that team-work is a core-value in the Sacco and there was nothing with people interacting with the ICT staff. However, she contended that the relationship the claimant and Elkana was suspicious because they would spend hours in the ICT office talking in low voices or again be seen together in a car. The two were also new in the Sacco.
25. She reiterated that the claimant had super rights to create users and he gave rights to Informak to do their work of providing Documents Management System (DMS). However, she admitted that investigation on the attack was still on going.
26. RW2 is Mr. Henry Mburugu, the ICT Manager of the Sacco. He also adopted his written statement as evidence. In brief, he testified that the claimant, as the Head of ICT, had privileged rights over the Sacco system including power to delegate the same rights. He stated that, after the fraud, a DW Agent was found in the machines after the fraud incidence.
27. He explained that a DW Agent is an application stored in a machine to enable the user access the machine remotely. The DW Agent was done using DMS user which was created by the claimant to facilitate Informak to extract existing users from the System and then disable it after finishing the work. A user password expires after 40 days as per the ICT policy. He contended that another user account named admin 1\$ was also discovered and he contended that only the claimant could access the DMS server to create it.



28. On cross examination, he confirmed that he took over the claimant's role but his position never changed from ICT manager to Head of ICT. He holds a BSC degree in ICT. He admitted that while the claimant was away in Kitengela for a visibility study, he (RW2) was left in control of the ICT department. However, he contended that the claimant was still able to access the system remotely, (RW2) contended that he had no such rights.
29. RW2 admitted that there are logs that show that the DW Agent was installed on 14th May 2022 in the afternoon but he could not state the exact time. He further stated that after the fraud, only the claimant could access the system until when he was sent on compulsory leave. However, he admitted that there are no logs to show that the claimant deleted all the mess in the system.
30. He confirmed that the claimant was not the only one with the rights to create accounts but he maintained that the claimant is the one who created the DMS account. As regards the admin 1\$ account, he admitted that he had no evidence to prove that the claimant created that account. He further admitted that the whole system crashed before any investigation could be done on it.
31. He confirmed that the DMS from Informak started operating in 2022 before the fraud but that it was in its preliminary stage after the physical registry was set up. He contended that the claimant as the Head of ICT department, was the only one dealing with Informak. He admitted that during the disciplinary hearing he stated that it is the claimant who created admin 1\$ account but in his written statement herein, he stated that the account was in fact created by a third party. He confirmed that he did know how investigation by the police went on. Finally, he confirmed that the DW Agent was installed in both the main server and the DMS server.
32. RW3 is Nicholas Mutuma Murugi, an Accounts officer for the respondent. He also adopted as evidence his written statement dated 1st February, 2023. He testified that he used to interact with the claimant because he relied on ICT to input data in the system. On 14th May, 2022 he paid for goods at Nkubu market but he failed to receive a confirmation text. He then called the claimant because he was unable to pay for the goods. The claimant then reported the matter to the mobile banking. He then told him that there was no problem on his side and probably it was a delay in the system.
33. On 16th May, 2022, he learned from the claimant that the system had been compromised. The claimant then made an analysis report of the affected accounts. About Khs.7.3 million was lost in the fraud.
34. On cross examination, RW3 stated that the claimant had handled the fraud incidence properly. He admitted that he was part of the team that went for visibility study before Informak was procured. In his view, the procurement was properly done. He also testified that the claimant had super rights over the Sacco system but stated that he could not say that the claimant was involved in the fraud. He contended that the claimant actively tried to recover the lost money.
35. RW4 is Mr. Aziz Yusuf Wachira, a technical consultant at Calwide Solutions which provides support to the respondent in case of an issue. He is a programmer. He testified that on 15th May 2022, the claimant told him over the phone that there was an incidence and they had shut down mobile services. He went to the Sacco on Monday 16th May 2022 and checked system logs. The Sacco has two servers, Navision server and DMS server.
36. He found the Navision server was the one compromised. The access to the system was from the DMS server. He then prepared a report which he produced as exhibit D.6.
37. On cross examination, he stated that his report was conclusive and it based on information from the Navision server. He contended that his role was to understand the logs and explain them to the client in a language they could understand. He then made recommendations which were acted upon.



38. He confirmed that while still working on the system with the claimant, someone logged them out meaning that someone had logged into the system using the same credentials. He contended that it was possible that person was the one who had done the attack. He opined that the claimant had acted professionally to salvage the attack, considering what he did after the incidence happened. He admitted that it was necessary to give Informak access to the machines allocated. Finally, he confirmed that he DW Agent was created on 14th May 2022 at 11.33 AM.
39. On reexamination, RW1 stated that he made observation in his report that there was existence of accounts with administrative privileges which were abused; and further that there was existence of admin accounts and their passwords on the DMS server. He stated that a DW Agent can be created remotely but in this case he could not tell whether it was created remotely or physically on the system.

Submissions

40. The claimant submitted that the respondents' witnesses did not adduce evidence to prove that he was involved in the system hacking that led to loss of money. He submitted that the defence witnesses including RW4 have admitted in evidence that it was necessary for him to create a temporary user accounts named YETU/ DMS to enable Informak to log into the computers allocated by the department and the server that they were configuring the system. He submitted that as per the security policy, the Informak were supposed to change the password upon the first login meaning that the account was solely in the hands of Informak. He maintained that the evidence on record shows that the fraud was caused by an attack connected to the DMS account created for Informak, who had sole control of as an independent vendor.
41. In view of the foregoing, the claimant submitted that the respondent has failed to prove valid and fair reason for the dismissal as required under section 45 of the *Employment Act*. He contended that the alleged negligence against him was not proved by evidence as the respondent failed to complete investigations on how the system was hacked. Therefore, he submitted that his dismissal was not justified.
42. For emphasis, he relied on *Allfayo Jagona Imbuya v Board of Management Ivugwi Secondary School (2018) eKLR* and *Pius Machafu Isindu v Lavington Security Guards Limited (2017) eKLR* where it was held that an employer must prove the reason for termination under section 43 of the *Employment Act* or the termination is deemed unfair under section 45 of the *Employment Act*.
43. The claimant submitted further that his dismissal was not done in accordance with fair procedure as provided by section 41 of the said Act. He contended that he was not invited to any disciplinary hearing to answer any charges. According to him, he was only invited for a discussion of the Cyber-crime incident that had occurred.
44. He contended that he diligently communicated his unavailability on 14th June, 2022 and requested for a rescheduling of the meeting but he received no response. His appeal was also never determined as no decision was communicated. Consequently, he submitted that the mandatory procedure for conducting disciplinary provided by the *Employment Act* was violated. For emphasis he cited *James Ondima Kabes v Trojan International Limited (2017) eKLR* where the court held that the employee is supposed to have his employee in the presence of another employee, and the employee is entitled to be given ample time to prepare for the hearing.
45. Finally, the claimant testified that he is entitled to the reliefs sought because his dismissal was unfairly done and it was malicious.



46. The respondent, on the other hand, testified that the claimant as Head of ICT, was in fact responsible for the overall security and integrity of the system. It further submitted that the claimant had indeed enabled Informak (DMS System vendor) to access the Sacco main server (Navision server) by creating a “DMS User”) namely admin 1 for the vendor in the main server. By creating the said user account, the claimant gave the vendor access to the main server.
47. It further submitted that the attack on the system happened when another user admin 1\$ was created on 14th May 2022 in the Sacco server using DMS (DW Service) application on both Navision and DWS server. It maintained that only the claimant had super rights to create that kind of users. It further maintained that the claimant had the rights to access the system remotely and therefore he cannot escape blame by merely alleging that he was away from the office when the malicious user was created.
48. To fortify the foregoing submission, the respondent pointed to the claimant’s report (Exhibit 14) where he stated that the creator of admin 1\$ user account and the logins to the Sacco server was done remotely on 14th May 2023 at 14.55 hours. It further submitted that the other ICT staff in the Sacco did not know whether the claimant had created the DMS account for Informak, and that the claimant gave Informak unlimited access. Consequently, the respondent maintained that either the claimant created the admin 1\$ account personally, or gave access to an unauthorized third party who created it and used it to access the Sacco server to commit the cyber-crime.
49. It further submitted that the claimant did not join Informak as a party to the suit and as such he is estopped from trying to blame Informak without any pleadings to that effect. In the respondents’ view, parties are bound by their pleadings and therefore Informak cannot be condemned unheard.
50. As regards the procedure followed, the respondent submitted that the claimant was invited for a disciplinary hearing before a committee but he failed to attend for no reason. Consequently, it submitted that the dismissal was fair and the claimant is not entitled to the reliefs sought.

Issues for determination

51. There is no dispute that the claimant was employed by the respondent as its Head of ICT. It is also a fact that the claimant created DMS user account named YETU/DMS for Informak to facilitate its personnel access the Sacco computers allocated and Server in order to install the DMS which they were contracted to install. It is further a fact that the respondents’ main server (Navision server) was compromised on 14th May 2022, when malicious users were created and used to defraud the Sacco funds. Finally, it is a fact that the claimant was dismissed for being either the person who attacked the system or for negligence that caused the fraud. The issues for determination are:-
 - a. Whether the reason for the dismissal was valid and fair.
 - b. Whether a fair procedure was followed.
 - c. Whether the claimant merits the reliefs sought.

Reason for dismissal

52. The dismissal letter was not produced as exhibit for the court to see the exact reason for the dismissal. Therefore I have gathered it from the pleadings, evidence and submissions that, the reason for the dismissal was either that the claimant committed the fraud himself or caused the fraud through negligence performance of duty by giving Informak access to the Sacco server.
53. I have considered the evidence adduced by both sides and it points to the fact that the attack on the main server was connected to the DMS user account, YETU/DMS, that was created by the claimant



for Informak to facilitate it do the work it was contracted by the respondent to do. Both the claimant, and the defence witnesses agreed that the DMS user account was necessary for Informak staff to access the computers allocated and the server to do the work it was contracted to do.

54. There is also evidence from both side that, the claimant had the right under his employment contract to create such user accounts. Consequently, the creation of the YETU/DMS user account was lawful. The claimant’s evidence, that after Informak changed password, he had no control over the DMS account has not been rebutted. The possibility that the malicious attack on the system was done by or caused by the negligence of Informak has also not been ruled out as no conclusive investigations were done before the whole system collapsed after the fraud.
55. It follows that the respondent has failed to prove on a balance of probability that the claimant committed the said attack and the fraud, or that he caused it through his negligence. It is easy to accuse him of failure to ensure security of the system but then the respondent has not shown that there was lack of security. In fact, the report by Calwide Solutions Limited did not implicate the claimant. Likewise, the police investigations were said to be still on going. Consequently, I find and hold that the reason for dismissing the claimant was not valid and fair. In the case of *Pius Machafu Isindu v Lavington Security Guards Ltd*,^{supra}, the court held that:-

“...the employer must prove the reason for termination (section 43); prove the reasons are valid and fair (section 45); prove that the grounds are justified (section 47 (5)), among other provisions...”

Procedure followed

56. Section 41 of the *Employment Act* provides that:-
- “(1) Subject to section 42(1), an employer shall, before terminating the employment of an employee, on the grounds of misconduct, poor performance or physical incapacity explain to the employee, in a language the employee understands, the reason for which the employer is considering termination and the employee shall be entitled to have another employee or a shop floor union representative of his choice present during this explanation.
- (2) Notwithstanding any other provision of this Part, an employer shall, before terminating the employment of an employee or summarily dismissing an employee under section 44(3) or (4) hear and consider any representations which the employee may on the grounds of misconduct or poor performance, and the person, if any, chosen by the employee within subsection (1), make.”
57. In this case the claimant contends that he was not accorded fair hearing as provided by the provision above. He contends that he received letter dated 8th June 2022 on 11th June 2022 inviting him for a “discussion” on the fraud incidence that had occurred. He was then in Nairobi where he was doing personal work and fell ill.
58. He responded by email to the HR Manager requesting for rescheduling of the meeting but the request was ignored and the meeting went on as scheduled on 14th May, 2022. When he reported back on 23rd June 2022 from his compulsory leave, he was served with a dismissal letter dated 22nd June 2022 requiring him to clear with the Sacco. The respondent has however maintained that it invited the claimant for a disciplinary hearing and failed to attend deliberately and without sufficient reasons.



59. I have carefully considered the evidence and observed that the letter dated 8th June 2022 was captioned “Re: Invitation For Disciplinary Hearing.”

Consequently, I dismiss the allegation by the claimant that the letter only invited him for “a discussion” and not disciplinary hearing. In all fairness the letter was clear that the invitation was for disciplinary hearing and not mere discussion. In fact the correspondences filed by him shows that Jackline Wambui emailed to him a letter inviting him for disciplinary hearing, and he responded requesting for the “hearing” to be pushed for not more than a week because he was not available on 14th June, 2022.

60. On the other hand, I have observed that the claimant requested for rescheduling of the hearing date because he was not available o 14th June 2022, and further sought for particulars of the misconduct giving rise to the disciplinary proceedings in order to prepare for the hearing. The request was not baseless but founded on very solid grounds which were in line with his right to fair administrative action and the Rules of natural justice.

61. It is now trite law that before taking any adverse administrative action against an employee, the employer should give the reasons to the employee and then accord him a fair opportunity to defend himself. In my view, the claimant was entitled to know the particulars of the charges he was going to defend himself against in order for him to prepare effectively. The respondent was unreasonable by insisting on continuing with the disciplinary hearing on a day when the claimant was not available and by failing to provide the particulars of the misconduct to enable him prepare for the hearing.

62. In addition, the respondent acted unfairly by failing to entertain the appeal by the claimant. Instead it published his photo in a Newspaper to notify the public that he was no longer an employee of the Sacco before the appeal mechanism was exhausted.

63. Finally, the respondent acted unfairly by failing to issue the claimant with certificate of service after clearing with the Sacco, and further delaying payment of his terminal dues until the suit came up for hearing. Considering all the respondent’s conduct in handling the claimant’s case, I find and hold that the procedure followed before the dismissal was not fair. It violated the rules of natural justice as codified in Article 47 of *the Constitution*, and section 41 and 45 of the *Employment Act*.

64. Its clear that the claimant was not accorded fair hearing as required under section 41 of the *Employment Act*. He was not explained the particulars of his offence in the presence of a fellow employee of his choice and then allowed to defend himself.

Reliefs

65. In view of the finding above that the respondent has failed to prove a valid and fair reason for dismissing the claimant, and further that a fair procedure was followed, I make a declaration that the dismissal was unfair and unlawful as prayed.

66. Flowing from the foregoing, I find that the claimant is entitled to payment of salary in lieu of notice plus compensation for the unfair termination under section 49(1) of the *Employment Act*. His contract of employment provided for a notice period of 3 months which I award to him. In addition, I award him three months’ salary as compensation considering that he only served for about 2 years; and also that he did not cause his dismissal through misconduct.

67. The claim for gratuity is also granted. Although the HR Manual at clause 3.8.4 provides for the benefit to employees who complete 5 years continuous service, it is only fair for the court to award gratuity if the employee is prevented from completing the five years’ service by the employer through unfair and



unlawful dismissal. Therefore, I award him gratuity at the rate of one and a quarter times his monthly basic salary for every year of service completed.

68. The claim for salary for June, leave allowance and leave days lacks particulars but the court was told by the defence counsel that it was admitted. The court was also told by the claimant's counsel that the money was used to settle a Sacco loan guaranteed by the claimant. The foregoing was not part of the pleadings before the court and I will not be drawn to secondary disputes.
69. The claim for general damages for emotional and psychological torture, and publication of his photo in the Newspaper are declined. First the unfairness caused by the unfair termination has been adequately compensated under section 49 (1) of the *Employment Act*. Secondly, the publication of a photo to notify the public that the claimant had exited the Sacco is reasonable and permitted to warn people from dealing with the claimant on behalf of the Sacco. It is a good practice aimed at mitigating fraud in businesses.
70. The claim for certificate of service is allowed as prayed because it is a right under section 51 of the *Employment Act*.

Conclusion

71. In view of the declaration and the award made above, I enter judgment for the claimant in the following terms:-
 - a. Notice 2 x 75,800.....Kshs.151,600.00
 - b. Compensation 3 x 75,800.....Kshs.227,400.00
 - c. Gratuity 1.25 x 2 x 75,800.....Kshs.189,500.00
Kshs.568,500.00

The award is subject to statutory deductions but the claimant is awarded costs plus interest at court rate.

DATED, SIGNED AND DELIVERED AT NYERI THIS 29TH DAY OF SEPTEMBER, 2023.

ONESMUS N MAKAU

JUDGE

Order

In view of the declaration of measures restricting court operations due to the Covid-19 pandemic and in light of the directions issued by his Lordship, the Chief Justice on 15th April 2020, this judgment has been delivered to the parties online with their consent, the parties having waived compliance with Rule 28 (3) of the ELRC Procedure Rules which requires that all judgments and rulings shall be dated, signed and delivered in the open court.

ONESMUS N. MAKAU

JUDGE

