REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

ODPC COMPLAINT NO. 0497 OF 2024

KENNEDY WAINAINA MBUGUA..... COMPLAINANT

-VERSUS-

BOLT OPERATIONS OU AND

BOLT SUPPORT KENYA LIMITED .....RESPONDENT

DETERMINATION

(Pursuant to Section 8(1)(f) and 56 of the Data Protection Act, 2019 and Regulation 14 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021)

A. INTRODUCTION

1. The Office received a complaint on 19th March 2024 from the Complainant. The complainant alleges that the Respondent unlawfully accessed and processed his personal information, resulting in the unlawful disclosure of his personal data to third parties who used his Bolt driver account information for fraudulent purposes.

B. LEGAL BASIS

2. Article 31(c) and (d) of the Constitution of Kenya 2010 provides for the right to privacy. Consequently, as an effort to further guarantee the same, the Data Protection Act, 2019 (hereinafter as 'the Act') was enacted.

3. The Office of the Data Protection Commissioner (hereinafter 'this Office' or 'the Office') was established pursuant to Section 5 of the Act and is mandated with the responsibility of regulating the processing of personal data; ensuring that the processing of personal data of a data subject is guided by the principles set

out in Section 25 of the Act; protecting the privacy of individuals; establishing the legal and institutional mechanism to protect personal data and providing data subjects with rights and remedies to protect their personal data from processing that is not in accordance with the Act.

4. Section 8(1)(f) of the Act provides that the Office can receive and investigate any complaint by any person on infringements of the rights under the Act. Furthermore, Section 56(1) of the Act provides that a data subject who is aggrieved by a decision of any person under the Act may lodge a complaint with the Data Commissioner in accordance with the Act.

5. This determination is premised on the provisions of Regulation 14 of the Data Protection (Complaint Handling Procedure and Enforcement) Regulations, 2021 (hereinafter as 'the Enforcement Regulations') which states that the Data Commissioner shall, upon the conclusion of the investigations, make a determination based on the findings of the investigations.

C. BACKGROUND OF THE COMPLAINT

6. This Office received a complaint from the Complainant on 19th March 2024. The complaint was lodged pursuant to Section 56 of the Act and Regulation 4 of the Enforcement Regulations from the Complainant who is an aggrieved data subject.

7. Pursuant to Regulation 11 of the Enforcement Regulations, the Office, notified the Respondent of the complaint filed against it *vide* a letter dated 28th March 2024 and referenced ODPC/CONF/1/5 VOL 1 (905). In the notification of the complaint, the Respondent was informed that if the allegations by the Complainant were true, it was in violation of various provisions of the Act. Further, the Respondent was asked to provide this Office with the following: -

    a. A response to the allegations made against it by the Complainant;

    b. A contact person who can provide further details as regards to the complaint;

    c. Any relevant materials or evidence in support of the response;

d. The legal basis relied upon to process and engage with the Complainant's personal data;

e. A detailed description on whether they uphold the rights of data subjects as per section 26 of the Act and how the same is fulfilled;

f. Details of how they obtain, store and process personal data;

g. Evidence as to whether the complainant consented to processing of their personal data;

h. Any other relevant information they wish the Office to consider.

8. The Respondent responded to the notification of complaint letter *vide* a response dated 10th May 2024.

9. On 10th May 2024, the Office forwarded the Respondent's response to the Complainant and invited him to file a rejoinder to the same.

10. On 23rd May 2024, the Complainant filed a rejoinder to the Respondent's response.

11. The Office then conducted a site visit at the Respondent premises on 31st May 2024 further to which the Respondent availed a further response to the site visit questions on 8th June 2024 and 14th June 2024.

12. This determination is therefore as a result of analysis of the complaint as received, the response from the Respondent, the Complainant's reply to the Respondent's response and investigations conducted by the Office.

D. NATURE OF THE COMPLAINT

13. The Complainant alleges that the Respondent unlawfully accessed and processed his personal information, resulting in the unlawful disclosure of his personal data to third parties who used his Bolt driver account information for fraudulent purposes.

E. SUMMARY OF EVIDENCE ADDUCED

I. THE COMPLAINANT'S CASE

14. The Complainant alleged that on 15th May 2023 he was contacted by a lady known as W****** regarding his Bolt account. The said W****** informed the Complainant that his account was being used by a different driver raising concerns of unauthorized access and usage. In response to her request, the Complainant then sent selfies holding a newspaper along with his identification card number 2******3 in an attempt to regain control of his account.

15. The Complainant further avers that on 16th May 2023, despite several attempts he encountered difficulties logging into his Bolt account. He contends that his email and password were no longer recognized by the system. Subsequently, the Complainant discovered unauthorized rides being taken under his account totalling an implausible distance within a short timeframe. Despite multiple attempts to contact the Respondent for assistance, he received no response.

16. The Complainant also states that further investigations revealed that his Bolt account had been compromised with fraudulent rides being conducted under his identity. Moreover, the Complainant asserts that despite reporting the matter to both the Respondent and the police, there was no resolution. However, it is his claim that it was discovered that internal employees/agents of the Respondent were involved in the fraud and were terminated thereby supporting his privacy claim with the Office.

17. The Complainant argues that the Respondent compromised his privacy, exposed his account to fraud and failed to protect his privacy contrary to the Act.

18. The Complainant then requested the Office to write to the Respondent regarding the complaint and the need for immediate action, conduct a thorough investigation and ensure fair compensation.

19. The Complainant further adduced the following evidence to support his claim:

    a) Judgment in Appeal No: TLAB/E010/2023 dated 31st October 2023

b) Witness statement on the petition against the Respondent

c) Email correspondence between the Complainant and the Respondent

d) Screenshots of the Complainant's Bolt account with the Respondent

e) Screenshots of Whatsapp conversation between the Complainant and phone number +254 1*******4

d) Screenshots of messages allegedly from the Respondent to the Complainant.

II. THE RESPONDENT'S RESPONSE

20. The Respondent responded to the Complaint *vide* a letter dated 10th May 2024. In its response, on the first allegation of the Respondent unlawfully and illegally accessing and processing the complainant's personal data, the Respondent states that it takes unlawful access and processing of personal data seriously and that it is committed to upholding the standards under the Act. To demonstrate the level of compliance, the Respondent attached as annexure 1 the Privacy Notice for drivers to establish the lawful bases of processing personal data for specified purposes.

21. The Respondent further avers that the Complainant had been a registered and an active driver on the Bolt platform since April 2021 and thus understood that the Respondent would be processing his personal data when registering as such. As communicated in clause 3 of the said Privacy Notice for Drivers, the processing of the Complainant's personal data was necessary for the performance of Respondent's contract with the Complainant (enabling the complainant to provide transportation services on the Bolt app).

22. With regards to the Complainant's data subject rights under the Act, the Respondent observes that they did not receive any data subject rights requests from the Complainant to enable them to restrict, stop processing or otherwise delete the Complainant's personal data.

23. The Respondent also states that with regards to processing of the Complainant's personal data for fraudulent purposes, it unequivocally denies any involvement in fraudulent activities as the same was a result of malicious actors based on

information carried out by the Respondent's information security team absolving the Respondent or its agents of any complicity in the unauthorized access to the Complainant's account.

24. On the allegation that the Respondent compromised the Complainant's privacy, exposed his account to fraud and failed to protect his account as a Bolt driver, the Respondent observes that it has technical measures and a range of organization measures to protect the personal data it processes. It further reviews and updates the said measures from time to time.

25. The Respondent further observes that from its internal investigations, it did not suffer any data breach or compromise of its apps, systems or databases which could have led to the perpetrators accessing the complainant's account.

26. The Respondent still on the same allegation, alleges that its internal investigation revealed that the Complainant's incident was as a result of a phishing attack. Moreover, the Respondent avers that at the time the Complainant shared his personal data with the perpetrators the Respondent did not have a Kenyan Whatsapp Business account nor did it offer customer support services through the Whatsapp platform. The Respondent then highlighted the complainant's role as follows:

    a) The Complainant provided selfies while holding a newspaper along with his identification card. (Annexure A2.1)

    b) From the Complainant's bundle, he was requested to share his SMS confirmation code via Whatsapp on or around 15th May 2023. (Annexure A2.2)

    c) The Complainant appears to have shared his registered account password with the perpetrators over Whatsaap.(Annexure A2.2)

    The Respondent avers that the above disclosures effectively enabled the perpetrators to make a valid request to the Respondent's customer support team, reset his password, modify his city of operation on his bolt driver account and authorize a change in his international bank account details.

27. The Respondent further observes that there were failures on its customer support team. In this regard, the Respondent avers that it has global user

verification procedures in place that are designed to protect driver privacy when the Respondent receives requests relating to their accounts.

28. From its internal investigation, the Respondent avers that it identified some procedural oversights involving some if its customer support agents. On the account detail changes process failure, the Respondent avers that as it received the email change request by the perpetrators from an unregistered email address, the customer support agent should have prompted the sender to resend the account change request from the account's registered email address or via in-app message.

29. The Respondent further states that the outsourced customer support agent appears to have followed user verification guidelines that were not applicable globally, nor to the Kenyan Market. In doing so, the agent incorrectly advised the sender to share a selfie holding their valid government ID and a piece of paper showing the date of request.

30. Further, under the assumption that the Complainant had been verified, the outsourced customer agent then proceeded to submit an internal note to the Respondent's internal customer support agent to change the email address.

31. The Respondent further contends that there were escalation failures on the part of its customer support team. Moreover, the Respondent alleges that in the Complainant's case, the Respondent outsourced tier 1 customer support agent who failed to escalate the Complainant's grievances and requests to be contacted telephonically on 23rd May 2023 to an internal tier 2 customer support agent for further consideration. The Respondent further avers that while the Complainant did not explicitly request to speak to a manager, his requests were akin to the level of escalation.

32. The Respondent also alleges that the customer support team are trained to report all incidences regardless of its size. The Complainant having alleged that his account had been compromised, the Respondent's tier 1 customer support agent failed to escalate the case to the Respondent's internal tier 2 customer support agent and Bolt's privacy team. Further, the customer support agent manually blacklisted the perpetrator(s) devices used in the fraud between 16th

and 17th May 2023. However, the Respondent found no evidence of the agent having escalated the incident to the Respondent's Fraud, Information Security and Privacy teams.

33. On the allegation of the internal termination of Respondent's employees involved in the fraud, the Respondent avers that there is lack of evidence that the Respondent's employees were involved and absence of any employee terminations linked to the incident.

34. On the allegation of concerns raised regarding the potential number of drivers affected by similar fraudulent actions, the Respondent avers that they haven't received any other formal complaints lodged by the alleged affected drivers.

35. On the allegation of the Complainant of him making multiple attempts to contact the Respondent for assistance and receiving no response at all, the Respondent apologized on behalf of its customer support team for any inconvenience caused to the complainant by the perceived lack of response. The Respondent further submitted evidence of the Complainant receiving multiple responses from the Respondent between 15th May 2024 and 18th May 2024 and therefore the allegation is denied by the Respondent.

36. With regards to the allegation of the complainant reporting the issue to both the Respondent and the police and there being no resolution, the Respondent avers that in its investigation it identified certain procedural failures by the Respondent customer support agents. This included the failure to escalate the complainant's grievances to the Respondent's in-house customer support leads, the Respondent's Kenya's local operations team and the fraud, information security and privacy teams. The resultant effect was that the thorough investigations did not begin until receipt of the Office's Notification of the Complaint on 28th March 2024.

37. The Respondent further observes that it acknowledges that the Complainant did not receive an immediate resolution to his grievances. However, this was due to the Complainant initiating formal legal proceedings against the Respondent with the Transport Licensing Appeals Board in the midst of the incident as early as May 2023. The proceedings are subject to an ongoing appeal to the High

Court of Kenya. It is the Respondent's view that the litigation initiated by the complainant shifted the forum for resolution of his grievances from the Respondent's internal channels and procedures to those of Kenyan courts.

38. The Respondent also avers that on the same allegation, they cannot answer to the alleged inaction of the Kenyan police.

III. COMPLAINANT'S RESPONSE TO THE RESPONDENT'S RESPONSE

39. The Complainant enlisted some of the questions he had regarding the Respondent's response including how the perpetrators knew of his bolt details, how they accessed his account details, how they knew he was a bolt driver. He further avers that it is only the Respondent officials who can access his Bolt account details and approve changes like change of cash out contacts, change of the Bolt car in use, change of location, change of his driving license to a U.K driving license.

40. The Complainant further alleges that all the rides were back-to-back with each ride running for between 0-2 minutes while covering a distance of over 100km in less than 2 minutes which could be a clear indication that the same was a system generated ride that could only happen from the Respondent Office.

41. The Complainant asserts that all the 17 completed rides were all corporate rides whereby all the payments were paid from corporate client banks. He further alleges that it is only the Respondent who knows their corporate clients since upon registration, they furnish the Respondent with all the details where they will be deducting payments from after every corporate rides.

42. The Complainant further alleges that he started all the quoted texts from the Respondent after he had problems logging in to the Respondent account after his morning trip. Further, he claims that the Respondent is shying away from taking responsibility of having rogue staff who were later dismissed after his case escalated to court and thus the Respondent was found guilty from the Transport Licensing Appeals Board Tribunal in a case that ran from 18th May 2023 to 31st November 2023.

43. The Complainant observes that his account was suspended by the Respondent for 7 days after his complaint went to court and after the 7 days all the trips were deleted as shown in the evidences he presented. He further alleges that after the alleged suspension he was never again contacted by the Respondent on the issue.

44. The Complainant also asserts that all the money was cashed out to a different contact (Airtel line) which was changed during the fateful night and bore a different name which according to the Complainant contradicts the Respondent's argument because changing the cash out account, the Respondent must contact one.

F. INVESTIGATIONS UNDERTAKEN

45. The Office conducted a site visit at the Respondent's premises on the 31st May 2024. As a result, a series of questions were tasked to the Respondent in which they responded and further made a further response to the site visit questions on the 8th June 2024 as follows:

46. On the first question of the ability of the Respondent to demonstrate how drivers are onboarded to their system, the Respondent provided the onboarding process for drivers.

47. On the second issue of whether the Complainant was registered with the Respondent, the Respondent acknowledged that indeed the Complainant had completed his registration and is a registered driver with the Respondent. Further, that the Complainant has been registered since April 2021 and that the said account is currently suspended due to an existing debt on his account, outdated documentation and concurrent litigation proceedings in the High Court of Kenya.

48. On the issue of principle of accountability, the Office required a demonstration of audit trail/logs on the system. The Respondent presented on-screen logs during the said meeting. The Respondent further attached evidence in relation to the Complainant's Bolt account during the timeframe of the incident.

49. On the issue of rights of the data subject, the Respondent was required to demonstrate how they enabled the exercise of the said rights that were allegedly infringed. The Respondent observed that it upholds the rights of data subjects as provided for in the Act and that the said rights are communicated to Bolt's users though its local and global privacy notices. Further, that the Respondent has a dedicated Customer Support Team to handle the same requests also known as ('DSR') as they arise.

50. With regards to the Complainant's rights on the same issue, the Respondent avers that indeed the Complainant engaged in correspondence with the Respondent's Customer Support Team. However, due to a combination of the manner in which the Complainant's requests were phrased and human error on behalf of the Respondent's Customer Support Team, the Complainant's requests were not recognized as 'DSR' request. As a result, they were not handled in accordance with the Respondent's established DSR procedures.

51. With regards to the Complainant's right of access, the Respondent reiterates that the Complainant did not lose access to his Respondent driver account at any point during the incident, or after the incident.

52. With regards to the Complainant's right of rectification, the Complainant had requested for his vehicle, operation and driver's license to be updated on his driver account as he believed it had been wrongly changed. The Respondent stated that neither the Complainant's area of operation, nor his drivers license were changed on the Respondent's systems and are as originally inputted/selected by the Complainant as part of his registration to become a Respondent driver.

53. On the issue of how user accounts are monitored by the Respondent, the Respondent presented the Complainant's admin profile on-screen during the said meeting. They further observe that the accounts are securely accessed by the Respondent employees and authorised third parties through two-factor authentication and role-based access controls.

54. On the issue of whether the Respondent has an operational incident management plan, the Respondent provided an Incident Management Policy (IMP). Further, on whether the same was effected during the Complainant's incident, the Respondent asserts that due to procedural failures, the incident involving the Complainant was never escalated by Customer Support Agents at the time it occurred in May 2023 to the Respondent's Privacy and/or Information Security Teams for investigation and incident management. Therefore, the Respondent regretfully confirmed that the IMP and process for managing personal data breaches were not followed as they were designed to be at the time when the incident occurred.

55. On the issue of the internal investigations conducted by the Respondent on the Complainant's incident, the Respondent states that its Privacy team led a multi-stakeholder investigation into the complaint. The investigations launched by the Respondent in March 2024 included whether the systems had any technical vulnerabilities or suffered a data breach, how the phishing attack occurred, whether there are any procedural failures within Customer Support Team, evidence of Respondent employees being involved and the perpetrators impersonating the complainant.

56. Following ODPC's site visit, the Respondent conducted additional investigations to analyse a series of questions by the Office including the 17 trips taken by the perpetrators using the complainant's account on between 17-18 May 2023. The Respondent confirmed that the perpetrators performed 17 fraudulent trips using the complainant's account totalling to KES 26,250.

57. Further, on the Complainant's case, the Office needed verification as to whether any third parties were affected. The Respondent thus identified one passenger who may have been affected by the incident. The 17 fraudulent trips taken by the perpetrators appear to have been performed by the same passenger, who was a corporate user of the Respondent business client.

58. The Respondent asserts that they found no evidence of having suffered a personal data breach of its systems or that any of its personnel were responsible

were responsible for the unauthorized access into the passenger's account. Further, the Respondent has no records of any customer support tickets having been submitted to it to change the passenger account details in order to gain access to the passenger account. Also, refunds were issued to the Business client for all the fraudulent amounts debited from the passenger's Bolt business balance.

59. On the issue of how the perpetrators technically performed the 17 trips, the Respondent avers that form the available logs, it appears that the [redacted] that were all over 100km long, within very short periods of time. However, the Respondent confirms that it found no evidence of any of its employees being responsible for the "17 rides" and a such were not system generated rides as alleged by the Complainant.

60. On the issue of the Respondent attributing the Complainant's incident to a phishing attack, the Respondent avers that the Complainant's conduct, in which he shared his personal data and login credentials with an unauthorized third party was a catalyst to the said incident. Further, the Respondent monitors potential phishing attempts made *via* the Bolt in-app chat between drives and passengers. This initiative began in December 2023.

61. On the issue of whether the Respondent's investigation revealed any personal data was unlawfully accessed as a result of the incident, the Respondent stated that the perpetrators of the incident successfully logged into the Complainant's driver Bolt account and one third party data subject (a Bolt Business Passenger and user of the Bolt app).

62. On the specific personal data that was definitively accessed, the Respondent avers that it is still in the process of determining whether it has logs that can confirm what personal data was definitely accessed during the time the perpetrators had access to the Complainant's account.

63. On the specific personal data that was possibly accessed, the Respondent avers that on the driver account, the following data is a[redacted]

[redacted]

64. On the issue of whether the Respondent has conducted a risk analysis on its systems, the Respondent confirmed that it has conducted the same. It further availed Personal Data Breach assessment with regards to the Complainant's incident.

65. On whether the Respondent has conducted a Data Protection Impact Assessment on its high risk processing activities, the Respondent stated that a DPIA was not necessarily required or triggered by the incident and thus it has not conducted a DPIA for this incident. However, the Respondent confirms that it does carry out preliminary privacy risk assessments routinely and DPIAs where processing is likely to result in high risk to the rights and freedoms of the data subject.

66. On the measures put in place to ensure that the incident does not reoccur, the Respondent confirms that it has put in place certain measures such as awareness raising for Bolt drivers in Kenya, roll-out of two factor authentication on the Bolt driver portal in Kenya, updated procedure for drivers to change their email address among others.

67. The Respondent further availed its investigation report dated 14th June 2024. The findings of the said investigations according to the Respondent revealed that the incident was primarily caused by social engineering and third-party phishing techniques. Further, on the impact on the Respondent's systems, it was concluded that other than the personal user accounts of the Complainant and the Affected Passenger having been unlawfully accessed, there were no indications of a data breach or vulnerability of any Bolt apps, systems or databases as a result of the incident.

68. The Office has further reviewed the complaint as lodged, the Respondent's response, the Complainants reply to the Respondent's response and all the supporting documents provided by both parties.

G. ISSUES FOR DETERMINATION

69. It is not in contention that the Complainant's Bolt account was unlawfully accessed by unauthorized persons resulting in unauthorized rides being carried out which have been solely blamed on phishing attacks by the Respondent. Therefore, this Office will look into the issues in question and whether the same falls under the ambit of the Act.

70. In light of the above, the following issues fall for determination by this Office:

i. Whether there was a personal data breach with regards to the Complainant's incident;

ii. Whether there was infringement of Complainant's rights under the Act;

iii. Whether the Respondent fulfilled its obligations under the Act; and

iv. Whether the Complainant is entitled to any remedies under the Act and the attendant Regulations.

I. WHETHER THERE WAS A PERSONAL DATA BREACH WITH REGARDS TO THE COMPLAINANT'S INCIDENT

71. Section 2 of the Act defines "**personal data**" as any information relating to an identified or identifiable natural person. Similarly, the said section goes on to define "**personal data breach**" as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

72. The Complainant alleged that on 15th May 2023 he was contacted by a lady known as W****** regarding his Bolt account. The said W****** informed the complainant that his account was being used by a different driver raising concerns of unauthorized access and usage. In response to her request, the

Complainant then sent selfies holding a newspaper along with his identification card number 2******3 in an attempt to regain control of his account.

73. The Complainant further avers that on 16th May 2023, despite several attempts he encountered difficulties logging into his Bolt account. He contends that his email and password were no longer recognized by the system. Subsequently, the Complainant discovered unauthorized rides being taken under his account totalling an implausible distance within a short timeframe. Despite multiple attempts to contact the Respondent for assistance, he received no response.

74. The Respondent on the other hand, alleges that from its internal investigation the Complainant's incident was as a result of a phishing attack. Moreover, the Respondent avers that at the time the Complainant shared his personal data with the perpetrators, the Respondent did not have a Kenyan Whatsapp Business account nor did it offer customer support services through the Whatsapp platform.

75. Upon the Office's investigations, the Respondent averred that the specific personal data that was possibly accessed on the bolt driver account, includes the name and surname, email address, billing details, phone number, bolt earnings, bolt trip history, vehicle model and registration number, expiry dates of police clearance, PSV license, PSV insurance, NTSA inspection report and regular driving license, driving license number, payout account information, invoices, bolt balance reports and tax reports.

76. From the aforementioned information on the driver's account, the Office finds that information available on the driver's account such as name and surname, email address, phone number, vehicle model and registration number, driving license number, payout account information does constitute personal information as envisaged under Section 2 of the Act.

77. This Office shall not delve into the phishing aspect as claimed by the Respondent as this is not within the mandate of the Office. However, with regards to whether there was a personal data breach as stipulated under Section 2 this Office finds

that the aspect of unauthorized disclosure of the complainant's personal information to the alleged perpetrators does constitute a personal data breach.

78. The Office further takes cognisance of the Complainant's role in contributing to the personal data breach by sending his information to the alleged Respondent's employee known as W****** which started the whole chain of events that led to the personal data breach. From the evidence submitted by the Complainant, an aspect of the Whatsapp conversation to +254 *********, the said third party requests the Complainant to share his car documents for the Bolt account verification. The Complainant then responds *"I don't trust you anymore...prove to be u are a bolt staff, send me ur bolt id staff and your names....U logged me out jana and u changed all my bolt account details"*

79. In view of the foregoing, it is evident that the Complainant at some point during the incident became apprehensive that he may not have been conversing with an employee from the Respondent with regards to the incident.

80. The Office finds that the incident does have an aspect of personal data breach which falls within its mandate. Further, the Office also finds that the Complainant indeed made a contribution to the said personal data breach by first not making a verification as to whether the said number indeed belonged to the Respondent and secondly by giving his personal information by providing his selfie holding a newspaper and his Identification number to the alleged perpetrators as had been requested.

81. The Respondent blamed the incident on social engineering and third-party phishing techniques, but its investigation report dated 14th June 2024 confirmed that the Complainant and affected Passenger's personal user accounts were unlawfully accessed, despite no indication of a data breach or vulnerability in any Bolt apps, systems, or databases.

82. From the above assertions and its investigations, the Office concludes that the Respondent, through its investigations, indeed became aware of the personal data breach as evidenced by its finding that the Complainant's and passenger's user accounts were unlawfully accessed and the said accounts have personal information belonging to both the Complainant and the passenger.

II. WHETHER THERE WAS AN INFRINGEMENT OF THE COMPLAINANT'S RIGHTS UNDER THE ACT

83. Section 26(b) of the Act provides for the right of a data subject to access their personal data in custody of data controller or data processor. The Complainant sent the Respondent an email requesting to be facilitated access to his personal data as he was unable to access his account.

84. The Respondent however opined that the Complainant did not lose access to his Respondent driver account at any point during the incident, or after the incident. From the evidence adduced by both parties and the investigations undertaken, it is evident that the Complainant was unable to access his account and the personal data therein, during the said period occasioning him to contact the Respondent to enable him access his account. Therefore, his right of access was not upheld by the Respondent in the circumstance.

85. Section 26(d) of the Act provides for the right of a data subject to correction of false or misleading data. The Complainant had requested for his vehicle, operation and driver's license to be updated on his driver account as he believed it had been wrongly changed. The Respondent stated however, that neither the Complainant's area of operation, nor his driver's license were changed on the Respondent's systems and are as originally inputted/selected by the Complainant as part of his registration to become a Respondent driver.

86. Despite the above Respondent assertions, from the investigations conducted and site visit, some of the information that had been changed from the Complainant account included the car details, payment account details and the type of car used from the Respondent's system as alleged by the Complainant.

87. Generally, with regards to the Complainant's rights, the Respondent through its response dated 10th May 2024, observed that it did not receive any data subject rights requests from the Complainant to enable them to restrict, stop processing or otherwise delete the Complainant's personal data.

88. Additionally, after the Office conducted a site visit on the 31st May 2024. The Respondent in its follow up response dated 14th June 2024 averred that with regards to the Complainant's rights, the Complainant indeed engaged in correspondence with the Respondent's Customer Support Team. However, due to a combination of the manner in which the Complainant's requests were phrased and human error on the part of the Respondent's Customer Support Team, the Complainant's requests were not recognized as data subject requests 'DSR' request. As a result, they were not handled in accordance with the Respondent's established DSR procedures.

89. In view of the foregoing, this Office finds that the Complainant's right to access under Section 26 (b) of the Act and correction of false or misleading data section 26(d) of the Act were violated by the Respondent.

III. WHETHER THE RESPONDENT FULFILLED ITS OBLIGATIONS UNDER THE ACT;

90. The Respondent is a data controller within the definition of the Act and therefore has obligations pursuant to the Act.

91. The Respondent had an obligation under Section 25 of the Act to ensure that the Complainant's personal data is, amongst others:

i. processed in accordance with the right to privacy;

ii. processed lawfully, fairly and in a transparent manner in relation to the Complainant;

iii. accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;

92. From its internal investigation, the Respondent avers that it identified some procedural oversights involving some if its customer support agents. For instance, on the account detail changes process failure, the Respondent avers that as it received the email change request by the perpetrators from an unregistered email address, the customer support agent should have prompted

the sender to resend the account change request from the account's registered email address or *via* in-app message.

93. The Respondent further states that the outsourced customer support agent appears to have followed user verification guidelines that were not applicable globally, nor to the Kenyan Market. In doing so, the agent incorrectly advised the sender to share a selfie holding their valid government ID and a piece of paper showing the date of request.

94. Further, under the assumption that the Complainant had been verified, the outsourced customer agent then proceeded to submit an internal note to the Respondent's internal customer support agent to change the email address.

95. From the above assertions, it is evident that the Respondent did not conduct the necessary verifications it needed to conduct before effecting the changes allegedly requested by the perpetrators. In that regard, it did not adhere to the principles of processing personal data espoused under Section 25 of Act thereby not fulfilling its obligations in that regard.

96. Section 31 provides for the Data Protection Impact Assessments where a processing operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes, a data controller or data processor shall, prior to the processing, carry out a data protection impact assessment.

97. Upon investigations, the Respondent revealed that a DPIA was not necessarily required or triggered by the incident and thus it has not conducted a DPIA for this incident. However, the Respondent confirms that it does carry out preliminary privacy risk assessments routinely and DPIAs where processing is likely to result in high risk to the rights and freedoms of the data subject. The Office noted from the investigations that a DPIA has not been carried out for the account management systems with regards to drivers and passenger user accounts in Kenya.

98. Further, the Office finds that the Respondent conducts large scale processing of personal data in relation to the drivers and passenger's user accounts which is a prerequisite for a DPIA and therefore should be conducted.

99. Section 43(1) & (2) of the Act provides that where personal data has been accessed or acquired by an unauthorised person, and there is real risk of harm to the data subject whose personal data has been subjected to the unauthorised access, a data controller shall notify the Data Commissioner without delay, within seventy two hours of becoming aware of such breach.

100. The Respondent failed to fulfil this obligation as they did not provide any evidence that they reported the subject personal data breach to this Office, nor did they provide an explanation as to whether or not an assessment was conducted to determine whether the same was a notifiable data breach, as per Section 43 as read with Regulations 37 & 38 of the Data Protection (General) Regulations.

101. Section 41 of the Act provides that every data controller or data processor shall implement appropriate technical and organisational measures which are designed to implement the data protection principles in an effective manner; and to integrate necessary safeguards for that purpose into the processing. Further, to give effect to this section, the data controller or data processor shall consider measures such as;

(a) to identify reasonably foreseeable internal and external risks to personal data under the person's possession or control;

(b) to establish and maintain appropriate safeguards against the identified risks;

(c) to the pseudonymisation and encryption of personal data;

(d) to the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(e) to verify that the safeguards are effectively implemented; and

(f) to ensure that the safeguards are continually updated in response to new risks or deficiencies.

102. Following ODPC's site visit and the Respondent's investigations, the Respondent confirmed that the alleged perpetrators performed 17 fraudulent trips using the complainant's account and personal information totalling to KES 26,250.

103. Despite the alleged perpetrators gaining from the Complainant's account, the Respondent asserts that they found no evidence of having suffered a personal data breach of its systems or that any of its personnel were responsible were responsible for the unauthorized access into the complainant's passenger's account. This allegation offends Section 41 of the Act which enjoins the Respondent, as a Data Controller to put in place the appropriate organizational and technical safeguards to effectively implement the data protection principles.

104. From the foregoing, this Office finds that the Respondent did not fulfil the above obligations as set out under the Act and the attendant Regulations.

IV. WHETHER THE COMPLAINANT IS ENTITLED TO THE REMEDIES UNDER THE ACT

105. Pursuant to Regulation 14(2) of the Enforcement Regulations, a determination shall state the remedy to which a complainant is entitled. Further, the remedies are provided for in Regulation 14(3) of the Enforcement Regulations.

106. The Complainant prayed for compensation in the form of general damages for losses incurred as a result the incident.

107. Section 65 of the Act provides for compensation to data subjects and states that, *"a person who suffers damage by reason of a contravention of a requirement of the Act is entitled to compensation for that damage from the data controller."*

108. Section 65(4) of the Act states that, "*damage includes financial loss and damage not involving financial loss, including distress."*

109. Further, Regulation 14(3)(e) of the Enforcement Regulations provides that the Data Commissioner may make an order for compensation to the data subject by the Respondent.

110. In considering whether to issue compensation, the Office will consider the finding on infringement of the rights of the data subject such as the complainant's right to access of his personal data contrary to Section 26(b) of the Act and the right to correction of false and misleading data contrary to Section 26(d) of the Act as espoused above.

111. From the foregoing, the Respondent is hereby **ordered to pay the Complainant Kenya Shillings Five Hundred Thousand Shillings only (KES. 500,000)** as compensation for the violation of the Complainant's rights under the Act.

112. Having found that the Respondent violated the Complainant's rights provided for under the Act and did not fulfil its obligations provided for under the Act, an enforcement notice shall be issued to the Respondent.

H. FINAL DETERMINATION

113. The Data Commissioner therefore makes the following final determination;

i. The Respondent is hereby found liable for violating the Complainant's right to access his personal data under Section 26 (b) of the Act, correction of false or misleading data under Section 26(d)of the Act and the failure to fulfil its obligations under the Act.

ii. The Respondent is hereby ordered to pay the Complainant **Kenya Shillings Five Hundred Thousand Shillings only (KES. 500,000)** as compensation.

iii. An enforcement notice to hereby issue against the Respondent.

iv. Parties have the right to appeal this determination to the High Court of Kenya within thirty (30) days.

DATED at **NAIROBI** this 17th day of June 2024.

IMMACULATE KASSAIT, MBS

DATA COMMISSIONER