REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

ODPC COMPLAINT NO. 1244 OF 2025

AADITI RAJPUT.....COMPLAINANT

-VERSUS-

DIAMOND TRUST BANK KENYA LIMITED.....1ST RESPONDENT

DIAMOND TRUST BANK UGANDA LIMITED .....2ND 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 Complaint alleges the improper disclosure of a third party's financial data to the Complainant. The Complainant additionally claims that as a result, she has lost access to her own DTB Bank statements and notifications since May 2025, causing financial difficulty in tracking her transactions.

B. LEGAL BASIS

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

3. The Office of the Data Protection Commissioner (hereinafter 'this Office' and/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 (Complaints Handling Procedure and Enforcement) Regulations, 2021 (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 the 25th August 2025. The complaint was lodged pursuant to Section 56 of the Act and Regulation 4 of the Enforcement Regulations from the Complainants who were the aggrieved data subjects.

7. Pursuant to Regulation 11 of the Enforcement Regulations, the Office notified the Respondents of the complaint filed against it *vide* a letter dated 8th September, 2025 referenced ODPC/CIE/CON/2/1(605) to the 1st Respondent and a Notice to enjoin the 2nd Respondent dated 30th September 2025 and referenced ODPC/CIE/CON/2/3(126). In the notifications of the complaint, the Respondents were informed that if the Complainant's allegations were true, they would be in violation of various sections of the Act. Additionally, the Respondents was asked to provide this Office with the following:

a) A response to the allegations made against them by the Complainant;
b) A contact person who can provide further details as regards this complaint;
c) Any relevant materials or evidence in support of their response above;
d) The lawful basis relied upon to use the Complainant's personal data;
e) A detailed procedure on how data subjects can exercise their rights;
f) Proof if any showing that the Complainant consented to her personal data being processed and linked to the 2nd Respondent.
g) The mitigation measures adopted or being adopted to address the complaint to the satisfaction of the Complainant, if any;
h) Any other information you wish the Office to consider.

8. The 1st Respondent responded to the allegations made against it *vide* a letter dated 16th September, 2025.

9. The 2nd Respondent responded to the allegations made against it *vide* a letter dated 21st October 2025.

10. In the interest of fair justice, and pursuant to Regulation 11 of the Data Protection (Complaints Handling Procedures and Enforcement) Regulations, 2021, the Office further informed the Respondent of the options of -

a. Reviewing the complaint and summarily resolving the same to the satisfaction of the Complainant, or

b. Resolving the complaint through mediation, negotiation and/or conciliation, as the alternative dispute resolution (ADR) mechanisms provided for by the Act and the Regulations.

D. NATURE OF THE COMPLAINT

11. The Complaint concerns the improper disclosure of a third party's financial information to the Complainant. After additional investigation, Diamond Trust Bank Kenya determined that the third party's account statements were sent by Diamond Trust Bank Uganda. The Complainant additionally claims that as a result, she has

lost access to her own DTB Bank statements and notifications since May 2025, causing financial difficulty in tracking her transactions.

12. The Complainant further claims that the relationship to DTB Uganda has caused her to lose trust in DTB Kenya's processes and controls because she has never visited Uganda. Finally, the Complainant alleges that despite many reports, the problem began in 2022 and has not been resolved until 2025.

E. SUMMARY OF RELEVANT FACTS AND EVIDENCE ADDUCED

i. THE COMPLAINANTS' CASE

13. The Complainant alleges that she had been receiving sensitive financial information belonging to a third party without the third party's knowledge. Further, the Complainant alleges that the ongoing failure by DTB to act despite her repeated reports has caused distress, anxiety, and loss of trust in their systems and controls.

14. The Complainant asserts that her account has been linked to DTB Uganda yet she has no relation and has never visited Uganda nor held any account with them.

15. The Complainant also states that there is a risk that her own sensitive banking data may have been misdirected in the same way as the third party's data, potentially exposing it to third parties. The Complainant asserts that unauthorized access to her financial data could lead to identity theft, fraud, or misuse of personal and financial information.

16. The Complainant indicates that the continued mishandling of her data by DTB undermines confidence in the security of Kenya's financial systems and poses a systemic risk if such errors are widespread.

17. The Complainant states that the issue has persisted since 2022 and worsened in 2025, despite multiple reports and she is currently not receiving her own statements, which she urgently requires for personal financial management and compliance purposes (e.g., record-keeping, tax, and audit needs).

18. The Complainant also avers that the ongoing, unresolved data leakage of another customer's statements constitutes a continuing breach, not a one-time incident and as a result she is seeking for immediate intervention necessary to prevent further harm to both herself and the any other affected customer.

19. The Complainant avers that she began receiving monthly bank statements addressed to a third party (a DTB customer unknown to her) in November 2022 and she reported the issue at DTB's Westgate Branch. The Complainant further avers that she was asked to share details, which she did, and was assured that it would be removed from the mailing list of this other account which never happened.

20. The Complainant claims that around March 2023 upon return from abroad, she reported the issue again at DTB's Diamond Plaza Branch and was again assured it would be resolved, but she continued receiving the wrong statements alongside her own.

21. In April 2025 the Complainant escalated the issue *via* email to DTB and they requested a sample of the emails she was receiving, which she shared.

22. On 8th May 2025, DTB confirmed *via* email that her address had been "removed from their records" and she immediately stopped receiving her own DTB statements and alerts altogether however, she continued receiving the third party's statements, including the most recent one on 1st August 2025.

23. Moreover, on 27th July 2025 the Complainant wrote again to DTB, raising both concerns (i.e., not receiving her own statements and continuing to receive the third party's statements and there was no response provided.

24. On the 29th July 2025 she sent a reminder and a ticket number was issued, but to date, no response or resolution has been provided. The statements she received come from no-reply@dtbafrica.com and the account in question belongs to DTB Uganda as detailed in the email.

25. The remedies sought by the Complainant include:

a) Immediate Corrective Action; that DTB be compelled to restore delivery of her own statements and communications without further delay and that her email address be permanently and securely delinked from the DTB Uganda account of the third party.

b) An assurance of Data Protection that DTB provide a written explanation of how her data was mishandled and what remedial measures have been put in place to prevent recurrence.

c) That ODPC ensures DTB implements stronger internal safeguards to uphold the Data Protection Act.

d) Compensation for the distress, inconvenience, and potential exposure of her personal and financial data outside Kenya and over an extended period, in line with the Data Protection Act which provides for such.

26. The Complainant further adduced the emails from the 2nd Respondent to her, that had financial data of the third party, and responses from the 1st Respondent to her when she lodged her complaint with them as evidence.

ii. THE 1ST RESPONDENTS' RESPONSE

27. The 1st Respondent submitted a response to the notification on 16th September 2025 averring that the Complainant first wrote to the Bank on 29th April 2025 advising that she had been receiving the account statements of the third party, and attached a copy of the Complainant's email dated 29th April 2025.

28. The 1st Respondent alleges that they responded to the Complaint on 30th April 2025, requesting a sample of the emails being received to enable the Bank to confirm and advise further to which they provided a copy of the Bank's email to the Complainant.

29. The 1st Respondent avers that on 1st May 2025, the Complainant shared a screenshot of a sample email addressed to the Third Party that she had received on her email address however, the screenshot did not have details of the sender.

30. Further, that on 8th May 2025, the 1st Respondent advised the Complainant that her email had been deleted from its database and at the time, the Bank could not trace any account in the name of the third party. Hence the bank IT team added the Complainant's email to its "Do Not Contact" list for e-statements as it tried to identify the root cause if the issue noting that the Bank did not have an account in the name of the third party.

31. It is noteworthy that the 1st Respondent's customer service and IT teams had no information as to whether the Complainant was an existing customer of the Bank by the time her account was added to the "Do Not Contact" list. Accordingly, the Complainant stopped receiving her own bank account statements, which are shared monthly. In her Complaint, the Complainant confirms that she had indeed stopped receiving her e-statements.

32. On 26th and 28th July 2025, the Complainant sent a fresh complaint advising that she had stopped receiving her e-statements, and she continued to receive the e-statements of a different person, the Third Party. However, the Bank's IT team could not establish why the Complainant continued to receive the e-statements of the Third Party who could not be traced on the Banks records and despite the Bank adding her email address to its "Do Not Contact" list.

33. Upon physical examination of the notification of the complaint that was received by the Bank from ODPC on 10th September 2025, the Bank established that the Third Party's account statements were being sent by Diamond Trust Bank Uganda ("DTBU"), a company which is incorporated in Uganda and a separate legal entity from the 1st Respondent. Whilst DTBU is a subsidiary of the Bank, the two entities maintain separate customer records and contacts details.

34. The 1st Respondent avers that the Complainant's correspondences to the Bank had nothing to indicate that the Third Party's account statements were being sent to the Complainant by DTBU. The email of 1st August 2025 from DTBU to the Complainant which has been attached to the Complainant's complaint was not shared with the

Bank. The Complainant has also never advised the Bank that the emails were being received from DTBU.

35. The 1st Respondent avers that while the Third-Party account statements were being sent by DTBU, they note that:

    i. The email from DTBU forwarding the Third Party's statements had DTBU's contact details if the Complainant had any queries or feedback which contacts are different from the Bank's contacts.

    ii. The Third Party's e-statements are password protected and the account number related to the statement has been hashed.

    iii. The email from DTBU had an "unsubscribe" option which the Complainant did not exercise. The 1st Respondent, however, appreciates that the Complainant may not have unsubscribed as she was under the mistaken belief that the Third-Party e-statements were being sent by the 1st Respondent and she wished to continue receiving the e-statements for her accounts with the 1st Respondent.

36. The 1st Respondent avers that they have since removed the Complainant's email from the Bank's "Do Not Contact" list. Further, they have also requested DTBU to delink the Complainant's email from the Third Party's banks accounts and request that the Complainant separately follows up with them *vide* the contact details indicated on DTBU's emails.

37. The 1st Respondent further stated that the Complainant is their customer and held accounts with the bank while the said third party was not their customer and hence did not exist in their database.

38. The 1st Respondent reiterated that the Complainant first reached out on 29th April 2025 about the issue, it stated that it wasn't in a position to verify and validate that the Complainant indeed physically visited its Office sometime back in 2021 due to the numerous clients who walk in on a daily basis.

39. The 1st Respondent stated that when the Complainant reached out to the call center in regards to the issue, its IT team had to add the Complainant to its "Do Not Contact List" this is the reason why she wasn't able to receive her own bank statements.

40. Upon being notified of the complaint by the Office, they wrote to DTB Uganda and requested them to delink the Complainant's email from the Third Party's bank accounts.

41. The 1st Respondent further stated DTB-Kenya and DTB- Uganda are two different entities and maintain separate customer records and contact details.

42. The 1st Respondent stated that it's possible that the incident was as a result of human error on DTB's Uganda side and not DTB Kenya.

II. COLLABORATION WITH THE PERSONAL DATA PROTECTION OFFICE - UGANDA

43. The Office requested for assistance from the Personal Data Protection Office of Uganda (PDPO) for purposes of initiating the investigation with regards to the 2nd Respondent as the entity is in their jurisdiction. As a result, the PDPO sent the 2nd Respondent a letter referenced PDPO/CI/003-CR and dated 13th October 2025 enclosing the Notice to enjoin the 2nd Respondent in order to compel the institution to send a response to ODPC.

44. Consequently, the 2nd Respondent *vide* a letter dated 21st October 2025 sent a response to the PDPO which is now included in the investigation.

III. THE 2ND RESPONDENTS RESPONSE

45. The 2nd Respondent provided a response *vide* a letter dated 21st October 2025. The 2nd Respondent avers that upon initial investigation, they established that the incident resulted from a human data entry error during customer onboarding.

46. Additionally, the 2nd Respondent confirms that the Complainant is not a customer of Diamond Trust Bank Uganda. The bank operates multiple systems that capture and manage customer data. In that regard, at the time of the incident, data was not flowing seamlessly between the Core Banking System and Customer Communication

Management System (CCMS) which extracts customer account statements from the Core Banking System and generates an email to the customer.

47. The 2nd Respondent avers that once the said complaint was brought to the Bank's attention in September 2025, the incorrect email was immediately deleted after the error was identified, and all misdirected communications ceased.

48. To prevent recurrence, the 2nd Respondent has now automated the flow of customer emails from the Core Banking System into the CCMS to eliminate manual data handling. Additionally, the Bank has launched an email validation project to verify and align customer email records between the two systems. This project is currently underway and is expected to be completed by December 31, 2025.

49. The 2nd Respondent further confirms that it has undertaken the following measures to ensure closure of the complaint involving the inadvertent transmission of account statements:

    i. The email address of Ms. Aaditi Rajput was immediately deleted from the Bank's systems.
    ii. The Bank has since enhanced its infrastructure to enable automated data flow across all platforms, thereby eliminating manual intervention in the capture of customer email addresses; and
    iii. Internal investigations have confirmed beyond reasonable doubt that the incident was an isolated error.

50. Furthermore, the 2nd Respondent avers that all email statements issued by the Bank are protected by security controls, including password encryption, which ensures that only the intended account holder can access the content. Account numbers are masked in the email message hence the recipient does not have access to the account number.

51. The 2nd Respondent further confirms that it has not processed any other data for the Complainant except her email which was captured erroneously and has since been

deleted from the Bank's systems. Furthermore, the Complainant is not a customer of the Bank.

52. The 2nd Respondent states that it has various communication channels which data subjects and customers use to exercise their various rights i.e., the official Bank email (info@dubuganda.co.ug), the Bank's official WhatsApp contact, the toll-free lines and the various social media platforms.

53. The 2nd Respondent confirms that it has not processed any other data for the Complainant except her email which was captured erroneously and has since been deleted from the Bank's systems. No consent was obtained or required, as no further processing of her personal data occurred.

54. The 2nd Respondent avers that they will continue to implement the following measures:

i. Masking of account numbers in all email notifications for account statements which ensures that no account number is exposed.
ii. Account statements are transmitted as PDF documents that are password protected, requiring the customers' unique password which is a customer number provided by the Bank.
iii. Each email statement includes an "unsubscribe" option which allows customers to opt out of receiving customer statements if they choose to.
iv. Maker checker process is followed for all customer data capture.
v. The Bank conducts regular staff training on data protection.
vi. Data Quality validations by the operations teams and control functions of the bank.

55. The 2nd Respondent further confirms that on October 20, 2025, the Head of Compliance, alongside Compliance officers and the Data Protection Officer (DPO) from Kenya, held a virtual call with the Complainant. The purpose of the discussion was to resolve the matter amicably and provide her with assurance regarding the steps the Bank has taken. During the call, 2nd Respondent apologized for the

inconvenience caused and detailed the specific controls now in place to ensure that such an issue does not recur.

56. The 2nd Respondent avers that the Complainant acknowledged the responses and requested a short period to reflect on the Bank's comprehensive reply. She committed to providing further feedback in writing to the DPO of the 1st Respondent.

F. INVESTIGATIONS UNDERTAKEN

57. In exercising its investigative mandate as provided for in the Act, this Office conducted internal investigations on all documentation submitted as well as a site visit to the 1st Respondent's premises on the 10th November 2025.

58. The 1st Respondent reiterated that the third party was not their customer and they did not know how the Complainant's data entered into the 2nd Respondent's system as they did not give them the said email and further, they do not have any existing integrations with the 2nd Respondent.

59. With regards to the question as to why the Complainant's complaint was not acted upon since 2022, the 1st Respondent stated that the same was speculative as they were unable to verify the records at the branch level since that is where the Complainant made the physical complaints. Further, it is difficult to know who the Complainant may have talked to due to high turnover and in addition CCTV is only stored for 12 months further making the verification difficult. The 1st Respondent could only speak to the complaint raised in 2025 by the Complainant that was captured by the system.

60. The 1st Respondent however confirms that the Complainant shared the screenshot depicting the 3rd party's email on 1st May 2025 and since the screenshot was not complete, they were unable to know where the third party's emails were originating from.

61. With regards to the principle of accuracy, the 1st Respondent averred that they only prevented the Complainant from accessing her e-statements temporarily as they were trying to establish root cause of the 3rd party emails to the Complainant.

Further, the 1st Respondent has alternatives where the Complainant could get the e-statements had she elected to.

62. The 1st Respondent further averred that they would present a detailed response to the site visit questions which the Office has not yet received as at the time of this determination.

G. ISSUES FOR DETERMINATION

63. It is undisputed that the 2nd Respondent sent the Complainant third-party account statements despite the fact that she was not their customer, but rather the 1st Respondent's. Furthermore, as a result, she has lost access to her own DTB Bank statements and alerts from the 1st Respondent since May 2025.

64. In light of the above, the complaint, the Respondents' responses and evidence adduced together with the investigations conducted, the following issues fall for determination by this Office:

i. Whether there was a violation of the Complainant's rights under the Act.
ii. Whether the Respondents fulfilled their obligations under the Act.
iii. Whether the Complainant is entitled to remedies under the Act.

I. WHETHER THERE WAS A VIOLATION OF THE COMPLAINANT'S RIGHTS UNDER THE ACT

65. Section 26 (a) of the Act provides for the right to be informed of the use to which a data subject's personal data is to be put.

66. The 2nd Respondent did not inform the Complainant that her personal data had been captured nor the purposes for which it was being processed. This violated transparency obligations requiring that individuals be informed at or before data collection. Because the Complainant was unaware her data was held or processed by the 2nd Respondent, she could not meaningfully exercise her rights.

67. Section 26 (b) of the Act provides for the right to access to the data subject where their personal data in custody of data controller or data processor. Regulation 9(4)

of the Data Protection(General) Regulations, 2021 provides that a data controller or a data processor shall comply with a request by a data subject to access their personal data within **seven** days of the of the request.

68. The Complainant adduced evidence showing that on the 27th July 2025 she requested to have her issue of not receiving her account statements(e-statements) resolved from the 1st Respondent. The Complainant further sent a reminder on the 29th July 2025 for the issue to be resolved and by the time the complaint was being lodged on the 25th August 2025, the same had still not been resolved.

69. The Office finds that by blocking the Complainant from receiving her own bank statements, the 1st Respondent violated the Complainant's right to access personal data held by a data controller. The wrongful suspension of her own statements impeded her financial management and compliance needs.

70. Further, Section 40(1)(a) of the Act provides for the right of rectification and erasure which states that a data subject may request a data controller or data processor to rectify without undue delay personal data in its possession or under its control that is inaccurate, outdated, incomplete or misleading.

71. Moreover, Regulation 10 of the Data Protection (General) Regulations 2021 provides that a data controller or data processor shall within **fourteen** days of the request, rectify an entry of personal data in the database where the data controller or data processor is satisfied that a rectification is necessary.

72. When the Complainant repeatedly reported the issue (from 2022 to 2025), the 1st Respondent failed to investigate the issue thoroughly, applied a remedy that did not address the core issue ("Do Not Contact"), and did not ensure rectification of inaccurate processing. The Office observes that the 1st Respondent failed to properly manage and resolve the complaint and further failed to take reasonable steps to rectify the inaccurate data processing thereby violating the right to rectification.

73. The Office observes that the 1st Respondent only acted upon being notified of the complaint by this Office, and took action to write to the 2nd Respondent to request them to delink the complainant's email from the Third Party's bank accounts.

74. From the foregoing, this Office finds that the Complainant's right to be informed under Section 26(a), right to access under Section 26(b) and the right to rectification and erasure under Section 40(1)(a) of the Act as read with Regulation 10 of the Data Protection (General) Regulations was violated by the Respondents as espoused above.

II. WHETHER THE RESPONDENTS FULFILLED THEIR OBLIGATIONS IN ACCORDANCE WITH THE ACT AND ATTENDANT REGULATIONS.

75. In addressing this issue, the Office will address the following questions:

a. *Whether the Respondents processed the Complainant's personal data in accordance with the principles of Data Protection.*

b. *Whether the Respondents established a lawful basis for processing the Complainant's personal data.*

c. *Whether the Respondents implemented appropriate technical and organizational measures to ensure data protection by design and by default.*

Whether the Respondents processed the Complainant's personal data in accordance with the principles of Data Protection.

76. Section 25 of the Act provides that –

Every data controller or data processor shall ensure that personal data is —

(a) processed in accordance with the right to privacy of the data subject;

(b) processed lawfully, fairly and in a transparent manner in relation to any data subject

(c)collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;

(f) 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;

77. Section 25 of the Act establishes the foundational principles governing processing of personal data. Both the 1st and 2nd Respondents, being licensed financial institutions, clearly fall within the statutory definitions of data controllers and, in certain instances, data processors as contemplated under Section 2 of the Act.

78. The 2nd Respondent confirmed that they processed the Complainant's email address with no legal basis. The Complainant's data was captured during customer onboarding for another person, a third party. The bank admitted that the processing resulted from a human data entry error and a system integration fault. Therefore, the processing without any lawful basis is contrary to the principle of lawfulness under Section 25(a) and (b) of the Act.

79. Additionally, the 2nd Respondent's inaccurate linking of the Complainant's account to another account which persisted for nearly three years, shows failure in accuracy by the 2nd Respondent in violation of Section 25 (f).

80. It is therefore the finding of this Office that both the 1st and 2nd Respondents herein, failed to process the Complainant's personal data in accordance with the principles of data protection enshrined in Section 25 of the Act.

Whether the Respondents established a lawful basis for processing the Complainant's personal data.

81. Section 30(1) of the Act provides for the lawful basis for processing of personal data. It prescribes that processing of personal data shall be lawful only if it satisfies one of the lawful bases enumerated therein i.e., that the processing is based on the data subject's consent; is necessary for the performance of a contract to which the data subject is party; is necessary for compliance with a legal obligation; is necessary to protect the vital interests of the data subject; or is necessary for the legitimate interests pursued by the controller or a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject.

82. The legal standard under this provision is not optional, rather, every data controller and processor must establish and demonstrate the specific lawful basis upon which personal data is processed. In this complaint, the 2nd Respondent failed to identify or substantiate any lawful ground justifying the collection and use of the Complainant's personal and sensitive financial data.

83. Accordingly, the Office holds that the 2nd Respondent herein failed to comply with their statutory obligations to ensure that the processing of the Complainant's personal data was supported by a valid lawful basis.

Whether the Respondents implemented appropriate technical and organizational measures to ensure data protection by design and by default.

84. Section 41(1) of the Act obligates that every data controller or data processor shall implement appropriate technical and organizational 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.

85. Regulation 32(j) of the Data Protection (General) Regulations, 2021 provides for the elements for the principle of integrity, confidentiality and availability states that having in place routines and procedures to detect, handle, report, and learn from data breaches is one of the means to secure data protection by design and by default.

86. Regulation 32(k) of the Data Protection (General) Regulations, 2021 further provides the element of regularly reviewing and testing software to uncover vulnerabilities of the systems supporting the processing under the principle of integrity, confidentiality and availability.

87. The data entry error was perpetuated by a systems integration failure between the Bank's Core Banking System and its Customer Communication Management System by the 2nd Respondent highlights a lapse in implementing appropriate technical measures to prevent errors from spreading, which is required under the principles

for data protection by design and default as provided under Section 41 of the Act and Regulation 32(k) of the General Regulations.

88. Sending third-party financial statements to an unintended recipient constitutes a breach of confidentiality and indicates insufficient technical and organizational measures. Although statements were password-protected, the disclosure of sensitive banking information including the identity of the customer and partial transaction information amounted to unauthorized disclosure and inadequate security safeguards. Furthermore, the duration of the breach demonstrates that the 2nd Respondent does not have procedures to detect, handle, report, and learn from data breaches in line with Regulation 32(j) of the General Regulations.

89. Additionally, Regulation 34 of the Data Protection (General) Regulations 2021 provides for the elements necessary to implement the principle of accuracy that includes:

(a)ensuring data sources are reliable in terms of data accuracy;

(b)having personal data particulars being accurate as necessary for the specified purposes;

(c)verification of the correctness of personal data with the data subject before and at different stages of the processing depending on the nature of the personal data, in relation to how often it may change;

(d)erasing or rectifying inaccurate data without delay;

(e)mitigating the effect of an accumulated error in the processing chain;

(f)giving data subjects an overview and easy access to personal data in order to control accuracy and rectify as needed;

(g)having personal data accurate at all stages of the processing and carrying out tests for accuracy at critical steps;

(h)updating personal data as necessary for the purpose; and

(i)the use of technological and organizational design features to decrease inaccuracy.

90. The 1st Respondent did not adhere to the principle of accuracy by activating the "Do not contact" step before verifying that the Complainant was their customer. On the other hand, the 2nd Respondent in linking of the Complainant's account to another account which persisted for nearly three years, shows failure in accuracy by the 2nd Respondent in violation of Regulation 34 of the General Regulations.

91. Based on the foregoing, the Office finds that the 2nd Respondent did not adhere to the technical and organizational measures to ensure data protection by design and default.

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

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

93. Having considered the merits of the complaint, the evidence adduced by both the Complainant and the Respondents, and having found that the 1st and 2nd Respondent violated the Complainant's right to be informed, to access and to rectification and erasure, it therefore, follows that there has been a violation of the Act by the said Respondents.

94. Section 65 (1) of the Act provides for compensation to a data subject 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. Section 65 (4) of the Act states that "damage" includes financial loss and damage not involving financial loss, including distress.

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

96. Having found that the 1st and 2nd Respondent violated Complainant's rights, the Respondents are hereby directed to compensate the Complainants as follows:

a) 1st Respondent – Kenya Shillings Two Hundred and Fifty Thousand (KES 250,000)
b) 2nd Respondent- Kenya Shillings Two Hundred and Fifty Thousand (KES 250,000)

97. Section 58 of the Act as read together with Regulations 14 and 16 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 further contemplates, as a remedy, the issuance of enforcement notices against an entity that has failed or is failing to comply with any provisions of the Act and the attendant regulations thereto.

98. This Office is guided accordingly, as a result an Enforcement Notice hereby ensues as against the 2nd Respondent.

H. FINAL DETERMINATION

99. In the ultimate, the Data Commissioner makes the following final determination;

i. The Respondents are hereby found liable.

ii. The 1st Respondent is hereby ordered to pay the Complainant **Kenya Shillings Two Hundred and Fifty Thousand (KES 250,000)** as compensation.

iii. The 2nd Respondent is hereby ordered to pay the Complainant **Kenya Shillings Two Hundred and Fifty Thousand (KES 250,000)** as compensation.

iv. An Enforcement Notice is hereby issued to the 2nd Respondent.

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

DATED at **NAIROBI** this 24th day of November 2025.

IMMACULATE KASSAIT, MBS
DATA COMMISSIONER