OFFICE OF THE DATA PROTECTION COMMISSIONER

ODPC COMPLAINT NO. 1454 OF 2024

JOSEPHINE EKATI ANINDO.....COMPLAINANT

-VERSUS-

NCBA BANK PLC.....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 Complainant alleges that she has received multiple unsolicited emails, including PIN/Password/OTP alerts, mobile transaction notifications, account statements, and promotional communications from Respondents, despite not being the rightful owner of the associated bank account and objecting to the processing of her personal data.

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 12th September, 2024. The complaint was lodged pursuant to Section 56 of the Act and Regulation 4 of the Enforcement Regulations by the Complainant who is the 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 8th October, 2024 referenced ODPC/CONF/1/5 VOL II (236). In the notification of the complaint, the Respondent was informed that if the Complainant's allegations were true, they would be in violation of various sections of the Act. Additionally, the Respondent 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 would provide further details regarding the complaint
   c) Any relevant materials or evidence in support of their response;
   d) How they obtained the Complainant's personal data;
   e) The lawful basis for denying the Complainant her right to object to the processing of her personal data, if any;

f) The mitigation measures adopted or being adopted to address the complaint to the satisfaction of the Complainant,

g) The mitigation measures adopted or being adopted to ensure that such occurrence mentioned in the complaint does not recur.

h) Any other information they wished the Office to consider.

8. This determination is therefore pursuant to the provisions of Regulation 14 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021.

D. NATURE OF THE COMPLAINT

9. The Complainant alleged that on diverse dates since March 2024, the Respondent processed her personal data in violation of data protection laws. She alleges that the Respondent repeatedly sent her unsolicited emails, including PIN/Password/OTP alerts, mobile transaction notifications, account statements, and promotional communications, despite not being the rightful owner of the associated bank account, and that additionally, the Respondent denied her the right to object to the processing of her personal data.

E. SUMMARY OF RELEVANT FACTS AND EVIDENCE ADDUCED

i. THE COMPLAINANTS' CASE

10. The Complainant alleges that since March 2024, she has been receiving multiple emails, including PIN/Password/OTP alerts, mobile transaction notifications, account statements, and promotional communications, despite not being the rightful owner of the bank account in question.

11. The Complainant avers that she made several attempts, particularly in July 2024, to request the bank to stop using the incorrect email address, but this issue remains unresolved.

12. Additionally, the Complainant states that she does not hold an account with the Respondent and has no prior knowledge of the accounts to which the information pertains. Consequently, she objected to the Respondent's processing of her personal data.

13. The Complainant alleges that despite the Respondent's commitment during a meeting on 23rd October 2024 to resolve the matter and ensure it would not recur, she continued to receive financial transaction details belonging to another individual on 26th October 2024. She asserts that the Respondent's assurances during the meeting, including offering merchandise as a goodwill gesture, have proven to be ineffective and raises concerns about the Respondent's complacency in addressing the issue.

14. The Complainant asserts that this recurrence demonstrates a failure on the part of the Respondent to uphold its commitment and to take adequate measures to resolve the matter conclusively. She pleads that the situation raises serious concerns about the security of personal data handled by the Respondent, questioning how many other clients might also be experiencing unauthorized disclosure of their sensitive information.

15. The Complainant further alleges that the Respondent's data entry personnel failed to exercise due diligence in distinguishing between her email address and the other party's email address. She contends that this oversight has perpetuated the issue, leading to her continued receipt of unintended emails containing sensitive transaction details of another individual.

16. The Complainant pleads that she has never received written communication from the Respondent to her correct email address and despite repeatedly confirming her address and raising objections. She also alleges that, contrary to the Respondent's claims of resolution, the problem has persisted, as evidenced by the transaction email received on 26th October 2024, just three days after the meeting.

17. The Complainant asserts that the Respondent's failure to address the matter adequately reflects a lack of adherence to its data protection obligations and demonstrates gross negligence in ensuring the accuracy and security of personal data.

18. As evidence, the Complainant adduced the following: -

    i. Copies of the account activity emails that she received from the Respondent; and

    ii. An email thread with the Respondent's, the Channel Support Agent, Contact Centre attempting to address the matter;

ii. THE RESPONDENT'S RESPONSE

19. The Respondent filed a response to the notification of the complaint on 28th October 2024.

20. In its response, the Respondent alleges that the email address j******@gmail.com was correctly associated with the account holder, J*****e A****o S*****e, as confirmed during the account opening on 22nd March, 2024. The Respondent states that this email address was provided by the legitimate account holder and has been maintained in the bank's system for necessary communications, including account statements, transaction alerts, and security notifications, in accordance with the bank's contractual and legal obligations.

21. The Respondent states that the processing of the email address was lawful under the Act, relying on contractual necessity, legal obligation, and legitimate interests. The bank asserts that the processing of the email address was required to fulfill its contractual obligations, including sending essential notifications related to the account, and to comply with legal requirements such as sending updates on terms and conditions, security alerts, and regulatory communications. The Respondent further asserts that its legitimate interest in maintaining communication with its customers supports the continued use of the email address.

22. On or about 6th June, 2024, the Respondent states that the customer confirmed the email address j*******e@gmail.com twice during a phone call when requesting a bank statement. The Respondent proceeded to send the requested statement to this confirmed email address. However, later that same day, the Complainant contacted the bank, stating she was not the intended recipient of the emails. The Respondent then conducted an investigation and confirmed that the

email address was still in use as the customer had not issued any instructions to remove it.

23. In response to the Complainant's objection, the Respondent pleads that on 9th October 2024, the bank re-verified the email address during a phone call with the customer, who again provided the same email address, albeit with some uncertainty. As a precaution, the Respondent disabled the email address from the customer's profile on 15th October 2024 and requested the customer to visit the branch to confirm the correct email address. The Respondent also reached out to the Complainant for a meeting to resolve the issue.

24. The Respondent states that, following a meeting held on 23rd October 2024, where the bank discussed its investigation and the actions taken, the Complainant expressed satisfaction with the resolution. The Respondent further alleges that the issue was resolved amicably.

F. INVESTIGATIONS UNDERTAKEN

25. After careful analysis of the evidence and applicable law, it was established that the email address provided by the affected customer during the account opening process varied from the Complainant's by a single letter.

26. The Respondent's allegations that it disabled the Complainant's email address from its internal systems are unmerited, as evidenced by the continued receipt of unwarranted emails by the Complainant with the latest instance reported on 26th November 2024, containing the Respondent's customer's personal data.

G. ISSUES FOR DETERMINATION

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

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

    ii. Whether the Complainant is entitled to remedies under the Act.

I. WHETHER THE RESPONDENT FULFILLED ITS OBLIGATIONS UNDER THE ACT

28. Pursuant to Sections 25(a), (b), and (f) every data controller or data processor shall ensure that personal data is processed in accordance with the right to privacy of the data subject, processed lawfully, fairly and in a transparent manner in relation to any data subject, and 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.

29. The investigations revealed that the Complainant's email address differed from that of the Respondent's customer's, indicating that the Respondent recorded inaccurate personal data.

30. Furthermore, upon being notified of this error by the Complainant, it became the Respondent's responsibility, to ensure compliance with Sections 25(f) of the Act. This would have required the Respondent to take immediate corrective action to prevent further violations and to safeguard the accuracy and integrity of personal data they were processing. This was not done.

31. Section 26(c) of the Act gives a data subject the right to object to the processing of all or part of their personal data.

32. Section 36 of the Act provides, that a data subject has a right to object to the processing of their personal data, unless the data controller or data processor demonstrates compelling legitimate interest for the processing which overrides the data subject's interests, or for the establishment, exercise or defense of a legal claim.

33. Furthermore, Section 40 of the Act provides, 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; or to erase or destroy without undue delay personal data that the data controller or data processor is no longer authorized to retain, irrelevant, excessive or obtained unlawfully.

34. The Respondent initially denied the Complainant's allegations, asserting that the email address in question was correctly associated with its customer and, therefore, it could not delete or erase the data. However, this position was later contradicted when it was confirmed that the email address recorded in the Respondent's system was different from the Complainant's, revealing an error in data capture.

35. Despite this, the Respondent engaged with the Complainant, assuring her that it would process her request for deletion and update the records with the correct details. However, based on the evidence furnished to this Office, these assurances remain unfulfilled.

36. In a rejoinder from the Complainant to the Office, evidence indicated that she still continued to receive emails from the Respondent, proving that the issue in contention remained unresolved. This failure to take corrective action, despite the consistent objection from the Complainant constitutes a clear violation of the Respondent's obligations as a data controller and processor under Section 25(f) as read with Section 36 and 40 of the Act.

37. Pursuant to, Section 41(1) of the Act, 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.

38. Sub-section (4) further provides; to give effect to Section 41(1), the data controller or data processor shall consider measures such as, to identify reasonably foreseeable internal and external risks to personal data under the person's possession or control, to establish and maintain appropriate safeguards against the identified risks, to verify that the safeguards are effectively implemented and to ensure that the safeguards are continually updated in response to new risks or deficiencies.

39. An analysis of the evidence unequivocally establishes that the Respondent did not take every reasonable step to ensure that personal data in its custody was

kept in a form which identifies the data subjects and that any inaccurate personal data is erased or rectified, in violation of the Act.

40. Based on the foregoing, the Office finds that the Respondent failed and/or neglected to fulfil its mandate as a data controller and processor processing personal data; subsequently, its actions resulted violation of the principles of data protection as envisaged under Section 25 (a), (b) & (f) and further occasioned a violation of the Complainant's right as envisaged under Sections 26(c), as read with Sections 36 and 40(1) of the Act.

II. WHETHER THE COMPLAINANT IS ENTITLED TO REMEDIES UNDER THE ACT AND HAS ESTABLISHED A BASIS FOR SUCH ENTITLEMENT

41. Pursuant 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.

42. As a remedy, the Complainant requested that the Office penalize the Respondent for the violation of her rights in accordance to the Act.

43. 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.

44. In light of the above, having found that the Respondent did not fulfill its obligations under the Act and as a result occasioning a violation against the Complainant, the Office hereby orders for an enforcement notice to be issued to the Respondent.

45. In so doing, this Office takes into account the nature and extent of violation with regard to the processing of the Complainant's personal data.

H. FINAL DETERMINATION

46. In consideration of all the facts of the complaints, the evidence tendered and the investigations conducted, the Data Commissioner makes the following determination:

i. The Respondent is hereby found liable.

ii. An Enforcement Notice is hereby issued to the Respondent herein.

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

DATED at **NAIROBI** this 11th day of December 2024

IMMACULATE KASSAIT, MBS
DATA COMMISSIONER