

IMPORTANT NOTICE: POTENTIAL SECURITY COMPROMISE INVOLVING PERSONAL INFORMATION

1. On 11 August 2026, we became aware of unauthorised access to an employee's email account within our information technology environment.
2. We immediately took steps to secure the affected account and commenced an investigation into the incident, which was substantially concluded, on 10 September 2026.
3. We have established that there was unauthorised access to the affected account during the period approximately 7 August 2026 to 11 August 2026. The affected email account provided access to certain information which may have included personal information relating to our clients and/or other data subjects.
4. The affected email account contained correspondence and documents relating to various matters and may have included personal information such as:
 - names and surnames;
 - contact details and email addresses;
 - identification numbers;
 - account and financial information;
 - information contained in FICA documentation;
 - information contained in lease agreements and related documentation; and
 - other personal information contained in business and operational correspondence.
5. Based on the investigation and the information currently available to us, we have not been able to establish with sufficient certainty which specific data subjects' personal information was accessed or acquired.
6. Our investigation was also unable to establish a definitive list of the individual data subjects whose personal information may have been accessible through the compromised account. We are nevertheless notifying you as a precautionary measure so that potentially affected persons are aware of the incident and can take any steps, they consider appropriate.
7. Following discovery of the incident, we took immediate steps to contain and investigate the compromise. These measures included:
 - securing the affected account;
 - restricting and terminating unauthorised access;
 - reviewing available access and audit logs;
 - investigating the nature and extent of the access;
 - reviewing the categories of personal information that may have been accessible;
 - implementing additional security measures to reduce the risk of a recurrence.
8. The potential consequences of the incident include the possibility that client information and the contents of emails may have been viewed or acquired by an unauthorised person. Depending on the nature of any personal information accessed or acquired, there may be a risk of fraud, identity theft or other misuse of personal information. We have no evidence at this stage of any misuse of personal information

9. On 14 August 2026 we reported the security compromise to the Information Regulator in accordance with section 22 of the Protection of Personal Information Act 4 of 2013 ("POPIA") and have provided the Regulator with the outcome of our investigation.
10. Based on the information currently available to us, we have no evidence confirming that your specific personal information was accessed, acquired or misused.
11. Nevertheless, as a precaution, we recommend that you remain alert to any unusual or unexpected communications requesting personal information, passwords, payment information or other confidential information.
12. You should not provide confidential information in response to an unsolicited communication and should verify any suspicious communication directly with the purported sender using independently obtained contact details. If you identify any suspicious activity which you believe may be connected to this incident, please contact us using the details below. We regret any concern or inconvenience that this incident may cause.
13. We take the protection of personal information seriously and have taken steps to investigate the incident, contain the risk and strengthen our security measures.
14. Should you have any questions regarding this notification or the security compromise, please contact:

Deputy Information Officer:	Lloyd Bell
Email:	Belll@dnpg.co.za
Telephone:	021 948 0934
15. We will provide further information should material new information become available.