Notification of security compromise in terms of section 22 of the Protection of Personal Information Act, 2013 (POPIA)

1 Simply Financial Services (Pty) Ltd ("**Simply**") is providing you with this notification in accordance with section 22 of the Protection of Personal Information Act, 2013 (POPIA).

2 This notice explains information security incident identified within our environment, the personal information that may have been impacted, and the steps you can take to protect yourself.

3 Simply takes the confidentiality, privacy, and security of personal information in its care extremely seriously. We have acted promptly to investigate the incident and strengthen the security of our systems, supported by independent digital forensic and legal specialists.

Overview of the incident

4 On 9 February 2026, an unauthorised third party used compromised user credentials to gain access to a reporting application (Metabase) hosted within Simply's environment. Through this access, the unauthorised party viewed and exported certain .csv data files made available within that application.

5 At this stage, our investigation confirms that the unauthorised access was limited to this application. There is no evidence that the unauthorised party accessed any other systems or underlying database.

6 Simply became aware of the incident on 23 February 2026 when evidence was received from the unauthorised third party indicating that personal information had been accessed. A technical investigation was initiated immediately, and the affected platform was taken offline for analysis, security hardening and access limitation measures.

Information potentially impacted

7 The personal information relating to you that may have been accessed depends on your relationship with Simply and the policy, membership, or administrative arrangements in place with your insurer or broker.

8 Based on our current forensic assessment, the information potentially affected may include one or more of the following categories of personal information:

(a) **Identification and demographic information**: first name, surname, initials, ID number (where held), date of birth, gender.

(b) **Contact information**: cellphone number, email address, home telephone number, postal address and/or residential address (where held).

(c) **Policy-related or membership-related information**: policyholder, insured life, beneficiary or member details; employer group (for certain membership records); policy or membership numbers; income, education, marital status and smoker status (where applicable to underwriting or quoting processes).

(d) **Company-related information (for group life policyholders only)**: where you are a policyholder under a group life or employee benefit arrangement, the information relating to your company that may have been accessed may include the company's registered name, trading name, registered address, company registration number and VAT number.

(e) **Beneficiary information**: first name, surname, contact details and, in some cases, ID numbers. Where a minor was listed as a beneficiary, the minor's information may also have been included.

(f) **Administrative or intermediary information**: details provided to or processed by the insurer, broker or other financial services partners through whom your policy, cover or membership was managed, including certain datasets relating to group schemes.

(g) **Banking details (limited category)**: only applicable where you had previously set up a debit order with Simply. In such cases, the fields may include bank name, branch code and bank account number. Importantly, if you did not provide debit order information to Simply, your banking details were not compromised.

Possible impact to you

9 As some of the personal information processed on the affected application includes identifiers such as names, contact details, date of birth, income-related fields, and, in some cases, bank account details, there is a possibility that affected individuals could face risks such as:

(a) Identity theft or impersonation attempts;

(b) Fraudulent or misleading contact attempts;

(c) Phishing or social-engineering attacks; or

(d) Attempts to obtain additional personal or financial information.

10 At this time, Simply is not aware of any misuse or public disclosure of the personal information potentially affected. Following the incident, Simply took steps to contain the incident and reduce the likelihood of further unauthorised use, and continues to monitor for any indications of misuse or publication.

What have we done

11 Immediately upon becoming aware of the incident, Simply:

(a) Took the affected application offline and undertook a full security hardening process;

(b) Restricted access to the platform to specific, verified geographic regions;

(c) Implemented precautionary rotation of credentials across core systems; and

(d) Reviewed and strengthened password and authentication requirements.

What can you do

12 We recommend that you remain vigilant and consider the following precautions:

(a) Be cautious when sharing your ID number, address, banking information, or other sensitive data online or with unfamiliar contacts.

(b) Always verify any request for personal information and only disclose it where you are satisfied that the request is legitimate and necessary.

(c) Avoid clicking on unfamiliar links or opening attachments from untrusted or unexpected sources.

(d) Change your passwords regularly and use strong, complex passwords that are unique to each account. Consider using a password manager to generate and securely store strong, unique passwords. If you use the same password across multiple services, update these to unique alternatives.

(e) Enable multi-factor authentication (MFA) for all online accounts, especially financial and email accounts.

(f) Ensure that your anti-virus and anti-malware software is active and up to date. Perform regular scans on your computers and mobile devices.

(g) Regularly check your credit report for any unusual or unauthorised activity. You may place a fraud alert with any of the major South African credit bureaus as an added precaution.

(h) If you are located in South Africa, you may apply for Protective Registration with the Southern African Fraud Prevention Service (SAFPS). This is a free service designed to help protect individuals whose personal information may be at risk.

(i) Online: https://www.safps.org.za/Home/OurServices_ApplyProtectiveRegistration

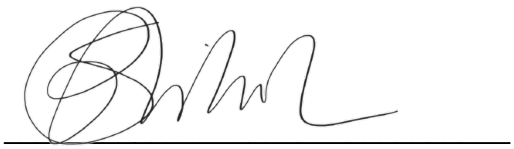
(ii) Email: Download the form from the SAFPS website and email the completed form with a certified copy of your ID or passport and proof of address to protection@safps.org.za.

(iii) SAFPS Call-Back Service: submit your details via the SAFPS website and an agent will contact you to assist with the process.

13 These measures are consistent with global best practices for data protection and personal information security.

14 If you have any questions or concerns about this incident or your personal information, please contact us at data@simply.co.za or 021 045 1513.

15 We recognise the importance of protecting your information and maintaining your trust. Simply remains committed to improving and strengthening its systems and safeguards to ensure the continued protection of personal information in its care.



Simon Nicholson

Information Officer

Simply Financial Services

Email: simon@simply.co.za