Unauthorised Third-party Access

Dear Data Subject,

We are writing to inform you of a cyber security compromise affecting Reflex Solutions, that is relevant to you. This notification is to empower you to understand any possible risks and how to best protect yourself.

Summary of the Incident

We have identified that an unauthorised third party gained access to our IT environment. Upon discovery, we immediately initiated our Incident Response Plan and engaged our specialist independent cyber security expert to jointly **(i)** contain the incident, **(ii)** determine the extent and the exposure, and **(iii)** prevent any further unauthorised access by any third party.

Our investigations verified that a limited amount of personal information had been accessed, which included **(i)** names, **(ii)** contact details, and **(iii)** email addresses.
At this time:

- there is no indication that your personal information has been misused;
- the accessed data appears limited in nature;
- we confirm that no financial information was accessed; and
- our experts continue to monitor the web for any evidence of the accessed data.

Steps that we have taken to address the incident

We initiated the Reflex Incident Response Plan, in which we:

- isolated affected systems and ensured containment of the incident;
- engaged external cybersecurity specialists;
- conducted full analysis to confirm scope;
- implemented protective measures to prevent further unauthorised access;
- strengthened system monitoring and security access controls; and
- notified the Information Regulator. The Information Regulator is the independent body established in terms of Section 39 of the Protection of Personal Information Act 4 of 2013 ("**POPIA**") to monitor and enforce compliance with POPIA. You can access the website at https://inforegulator.org.za/about/.

What this means for you and steps you can take to protect yourself

We strongly encourage you to remain vigilant and take protective measures against the potential adverse consequences flowing from the incident. We further encourage you to practice good digital hygiene based on the following (but not limited to) steps that can help reduce the risk of potential threats:

- stay alert against any suspicious calls, texts or emails that could be a scam or phishing attempts;
- be cautious of emails with spelling or grammatical errors, as these may be phishing attempts;
- avoid clicking on links or opening attachments from unknown or unexpected senders;
- use strong, unique passwords for your email account and never share passwords with anyone;
- ensure your browser and devices are regularly updated with the latest security patches; and
- never share your banking or credit card details unless you are certain of the request's legitimacy.
- If you suspect you have been a victim of fraud, report it to the South African Police Service on 0860 010 111:
    - The South African Cybersecurity Awareness Portal (SACAP) is a body established by the South African Government.
    - SACAP is a good source of cyber security information and tips: https://www.cybersecurityhub.gov.za/cyberawareness/.
    - The Financial Intelligence Centre also has some useful information on how to spot the warning signs of financial scams at https://www.fic.gov.za/scams-awareness/.

Our Commitment to You

Protecting your information remains a core priority. We apologise for any concern this may cause and reaffirm our commitment to maintaining the security of your information. If you have any questions, please reach out to us at databreach@reflex.co.za.

Thank you for your understanding and continued trust in Reflex.