Notification of security compromise

14 April 2022

Royal Bafokeng Holdings (Pty) Ltd ("**RBH**" / "**our**" / "**we**") provides this notification of an information security compromise it has experienced in terms of section 22 of the Protection of Personal Information Act, 2013.
RBH has determined that the compromise resulted in the unlawful access to and acquisition of data, including certain personal information stored within its IT environment, on or about 29 March 2022 ("**the incident**"). RBH has since taken the necessary measures to determine the scope of the compromise and to restore the integrity of its information system.

There is currently no indication that any personal information has been published or misused as a result of the incident, and RBH has taken active steps to trace the extracted data and to prevent its publication, including of personal information contained within the data.

Out of an abundance of caution, we are providing this information about the incident and the actions taken by RBH to mitigate its possible adverse effects.

Overview of the incident

RBH became aware of unusual activity on its servers where company data and some personal information is stored. A digital forensic investigation commenced immediately with the assistance of external specialists. That investigation has determined that data (including personal information) relating to RBH, its employees, directors and third parties, including some investee companies, was accessed and acquired unlawfully by an unknown and unauthorised third person(s) ("**the unauthorised party**").

What information was involved and possible consequences to data subjects

The full extent of the impacted data is at present difficult to ascertain as the unauthorised party partially disabled log tracking functionality on the programme used to extract the data.
We are however able to identify the following categories of personal information that may have been compromised:

1. Employee information such as:
    a. Employee username
    b. Password
    c. HR records detailing employees personal and financial information
2. Job applicant information such as:
    a. CVs of job applicants
    b. HR records detailing personal and financial information
3. Select Investee company information
4. jpg files which contained personal information such as:
    a. Images of employees, former employees, community members

To date, we are not aware of the publication or misuse of any personal information in relation to this incident. RBH is taking the necessary steps to report the incident to law enforcement and regulatory authorities in South Africa, including the Information Regulator.

Given the categories of personal information that may have been compromised, it is possible that any impacted personal information may be used to attempt fraud, such as social engineering / impersonation attempts, phishing attacks and/or email compromises.

We encourage you, as a precaution, to follow these security recommendations:

- Do not disclose personal information such as passwords and PINs when asked to do so by anyone via phone, fax, text messages or e-mail.
- Change your passwords regularly and never share these with anyone else.
- Verify all requests for personal information and only provide it when there is a legitimate reason to do so.
- Perform regular anti-virus and malware scans on your personal computer and mobile device, using software that is up to date.
- Do not click on any suspicious links.

What we have done

RBH takes the confidentiality, privacy, and security of information in its care very seriously. RBH acted promptly, through its attorneys, to issue a takedown notification to the cloud storage provider to which the data was extracted, and the account associated with the incident has been suspended.
RBH believes that the risk of any of the acquired data or personal information being published as a result of the incident is low.
While security safeguards are already in place to protect personal information in our control, RBH has deployed additional safeguards in order to ensure protection and security of information on our servers. These safeguards include, but are not limited to, enhanced anti-malware prevention and detection software.

For more information

If you have questions or concerns, please contact us at info@bafokengholdings.com.
Your trust is a top priority for us, and we remain committed to safeguarding personal information in our care.