July 2022

Important information regarding your information

Dear Tshiamiso Trust Claimant,

Notice of incident that may affect your personal information

I am writing to inform you of a data security issue which which we discovered on 23 June 2022 and which involved an unauthorised disclosure of limited personal information **that** you provided to us or that we have on record about you. We are contacting you as soon as we practically could after the Incident, and after completing our investigations, as per the requirements as set out in the *Protection of Personal Information Act*, 2013 (**POPIA**).

What happened?

Based on our investigation, it appears that on or about 23 June 2022, an Excel spreadsheet (**the Spreadsheet**) containing a list of persons who have lodged claims with the Tshiamiso Trust, which had been sent to the Eastern Cape Department of Health (**ECDOH**) on 15 June 2022, has been circulating via WhatsApp to multiple unknown parties.

Who did this?

As noted, this was not a compromise of the Trust's systems but rather that a person who may or may not have been authorised to receive this personal information shared the Spreadsheet without consent.

We continue to investigate the identity of the suspect. As is common with these incidents, it is not always possible to identify who is responsible for this malicious conduct. Should we identify the person responsible for sharing the Spreadsheet, we will work with law enforcement agencies and disclose the identity of the suspect only if law enforcement agencies think that it is appropriate to do so.

What information was involved?

The following categories of personal information which were contained in the Spreadsheet are as follows:

Name;

Industry number;

Identity number;

Passport number;

Bureau number;

Address;

Limited medical information relating to the status of a medical condition;

Claim number;

Claim status.

No financial information was included in the Spreadsheet. Additionally, we note that not all categories of personal information had been completed for each affected person. It therefore may be possible that of the above listed categories of personal information, the only information that was available on the list is a select combination of categories i.e. name, surname and address, and the medical information may not have been included.

What are we doing about it?

Our immediate concerns were, firstly, to determine how the breach occurred, and to ensure that no further personal information could be shared on an unauthorised basis. We immediately notified our forensic experts to investigate the source of the breach, and instructed our legal advisors on all necessary steps to take to ensure that the least amount of personal information possible is affected.

Our team of forensic specialists have worked tirelessly since 23 June 2022 to thoroughly investigate the Incident. We also sought advice from our legal advisors who have extensive experience in data protection matters. We have taken numerous steps and implemented all advice provided by our team of experts, which included the following:

- Requested the National Department of Health to investigate the breach on their end;
- Requested all unauthorised users to delete and retract the information, and communicated same to all our Service Providers who are aware of the incident;
- Heightened IT security measures, including encryption when sharing personal information and increased awareness and staff training; and
- Review of all contractual obligations to ensure appropriate data sharing agreements are in place.

The investigation remains ongoing.

Even though we were able to swiftly respond and mitigate cyber risk, we have instructed our forensic experts to identify any further mitigation steps that could possibly be taken by us to ensure the continued protection of information contained in our environment.

How could the information about you potentially be used?

While we have implemented the above measures to mitigate the possible adverse consequences of the Incident, it is possible that some of the personal information has been copied or retained by the unauthorised third party as a result of the Incident. At this stage it is clear that the information that may have been accessed is limited in nature. We are continuing our investigations with expert advisors; however, at this stage, it appears that there is minimal risk to affected data subjects. The possible impact is limited to access to and the use of the above-mentioned categories of personal information, some of which may already be publicly available .

What can you do?

At this stage, there is no action that you need to take. Although some of the information in the affected database may already be in the public domain,in order to mitigate the risk of identity compromise, you can register for a free Protective Registration listing with Southern Africa Fraud Prevention Service (**SAFPS**). The SAFPS is a non-profit organisation focused on fraud prevention and leads the fight against fraud and financial crime. The SAFPS assists in preventing fraud and impersonation as a result of identity theft to protect the public from the associated financial consequences. Its Protective Registration service alerts SAFPS members, which includes banks and credit providers, that your identity has been compromised and that additional care needs to be taken to confirm that they are transacting with the legitimate identity holder. Consumers wanting to apply for a Protective Registration can contact SAFPS at 011 867 2234.

Please do not hesitate to contact us at **080 1000 240** in the event that you require any further information concerning the Incident. You can also contact the Information Regulator at inforeg@justice.gov.za or via their website (www.justice.gov.za/inforeg) for more information.

We apologise for any inconvenience that may arise from this Incident.

Yours sincerely,

Mr. Daniel Kotton
Chief Executive Officer
Tshiamiso Trust