07 December 2022

NOTIFICATION REGARDING POTENTIAL COMPROMISE OF PERSONAL INFORMATION OF A DATA SUBJECT, IN ACCORDANCE WITH THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 (POPIA)

1. I refer to Section 22 (1) of Act 4 of the POPIA, titled **Notification of security compromises** which states that where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify—

    a) the Regulator; and
    b) subject to subsection (3), the data subject, unless the identity of such data subject cannot be established.

2. The POPIA states that the notification referred to in subsection (1) must be made as soon as reasonably possible after the discovery of the compromise, considering the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

3. BANKSETA would like to notify potential affected persons who are ''data subjects'' of the BANKSETA about a recent cybersecurity incident on the 10th of November 2022 in which some of its Information Technology (IT) systems were compromised through malware.

4. The BANKSETA analysed the nature and extent of the IT breach and has found that there might be personal information that has been accessed or acquired by an unauthorised person(s) or institution. No determination has been made of the identity of the perpetrators or institution. Furthermore, while the full extent of the compromised data is unknown at this stage, there was a potential 2,5TB of data in the affected IT systems. Part of this information included personal information such as names, identity numbers, contact and banking details.

5. One of the possible consequences of the breach is that personal information may be sold and used for unlawful purposes. In this regard, BANKSETA advises data subjects to take precaution by implementing some of the following mitigating measures:

    a) Review and authenticate your financial accounts, bank statements etc. to notice any suspicious transactions.
    b) Review and verify any suspicious communication relating to changes or requests for such changes to your personal information.
    c) Immediately contact the law enforcement institutions in the event of actual or suspected identity theft.

6. BANKSETA regrets the inconvenience caused by the cybersecurity breach of your personal information and has undertaken active steps to prevent and safeguard any further breaches on personal information placed in its care. Measures currently being implemented include the following:

    a) Isolation of the affected IT systems from the BANKSETA network while we investigate aspects of the IT breach.
    b) Improved Access control measures through stronger passwords and additional authentication features.
    c) Updating our antivirus and implementing network monitoring tools as well as reviewing security configurations of third-party firewalls for our hosted services.

7. Investigation on the cybersecuriy incident is continuing and BANKSETA will update data subjects on any further developments regarding the compromise of their personal information.

For queries, please send an email to ***Queries@bankseta.org.za***

Yours Sincerely,

Mr.Eubert Mashabane
Chief Excutive officer (CEO)