the doj & cd
Department:
Justice and Constitutional Development
REPUBLIC OF SOUTH AFRICA

To all data subjects

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

1. I refer to the above subject-matter and the requirement, in section 22 of the POPIA, that an identifiable data subject must be notified in instances where there are reasonable grounds to believe that the personal information of such a data subject has been accessed or acquired by an unauthorized person.

2. POPIA defines a data subject as a person to whom personal information relates, and the responsible party is defined as a public or private body which determines the purpose of and means for processing personal information. Therefore any person that has, in the course of interacting with the Department, submitted their personal information to the Department, is considered a data subject of the Department in terms of POPIA.

3. It is within that context that the Department wishes to notify potentially affected persons who are 'data subjects' of the Department about the other effect of the malware that attacked its Information Technology (IT) systems with effect from 05 September 2021.

4. Since the breach occurred, the Department analysed the nature and extent of the breach and has found that there might be personal information that has been accessed or acquired by an unauthorized person/institution, whose identity is currently still unknown. Although the full extent of the data that has been compromised has not yet been fully determined, it has been established that at least 1200 files have been exfiltrated (which might have contained personal information such as names, contact and banking details).

5. The possible consequences of the breach is the selling of the personal information and its use for unlawful purposes.

6. Therefore, as a precautionary measure, the Department would like all its data subjects to take note that access to the above-mentioned information may result in your personal information being used for unlawful purposes. Therefore, in order to mitigate the possible adverse effects of the security compromise, we recommend that you do the following:

    a. remain vigilant by reviewing your financial accounts, bank statements, etc;
    b. take special interest in bank notifications in terms of purchases made on accounts; and
    c. immediately contact the law enforcement in the event of actual or suspected identity theft.

7. The security compromise of your personal information is deeply regretted, however, In order to strengthen the security of information in its custody and to prevent a recurrence of a data security breach, the Department has put in place the following measures:

    a. Enhanced Access Control by way of strong password enforcement, Privileged Access Manager (PAM), and Virtual Private Network (VPN) access;
    b. Upgraded Defensive Measures, Including Third Party Firewalls, and Intrusion Prevention System (IPS), Security Event And Incident Monitoring (SEIM); as well as
    c. Upgraded its Anti-virus and Anti-malware Solutions on both server infrastructure and end-points.

8. The Department will ensure that all data subjects are kept up to date with regard to further investigations of the nature of the personal information that was compromised.

With kind regards,

ADV. D. MASHABANE
DIRECTOR–GENERAL
DATE: 04/10/21