LAW SOCIETY
OF SOUTH AFRICA

L.E.A.D® PROFESSIONAL AFFAIRS DE REBUS

14 October 2023

DRAFT NOTICE OF POTENTIAL UNAUTHORISED ACCESS OF PERSONAL INFORMATION[1]

Dear Data Subject,

This communication serves as a notice under the provisions of the Protection of Personal Information Act, 2013 (POPIA) aimed at informing you of a recent incident involving unauthorised access to personal information that may potentially affect you.

Although we have reasonable grounds to believe that personal information processed by the LSSA may have been unlawfully accessed, we are unaware of any unlawful use of such personal information.

The LSSA stores sensitive data of candidate attorneys and practitioners who register for educational services and products via our Legal Education Division [LEAD].

We confirm that the Information Regulator has been notified, as required in terms of section 22(1)(a) of POPIA.

It has taken us time to investigate via service providers, implement additional security measures and reinstate our cloud environment, and despite an assessment by the security advisors that they did interrupt the attack but were unsure of what information was accessed, we have worked on the possibility that there was a full data security breach, hence this detailed response.

INCIDENT RESPONSE:

In addition, the LSSA implemented the following measures to address the security compromise.

a. Shut down environments
b. Disabled compromised on-premises user account
c. Closed entry points
d. Established that the backups had data integrity until 6 September 2023
e. Used logs to build attack timeline
f. ALL passwords have been reset
g. Multi-factor authentication (MFA)

[1] To be sent after notification to Information regulator and confirmed receipt

h. Firewall
i. Endpoint detection and response (EDR)
j. Ensured that there was no 'locked access' to the data [Ransomware]

The following steps further amplified the above measures:

- Restoration of the compromised Production environment to the most recent backed-up date of 8 September 02h00.
- Rebuild the development environment;
- Cloud Environment Hardening and Network Resilience.
- Cloud User Access management Implementation; and
- Managed Detection and Response (MDR).

Upon further analysis and review, the following additional measures were introduced on 12 September 2023:

- Agreed to Cloud service provider's enabling on our MS Azure cloud - Security Operations Centre (SOC): A centralised unit that monitors, detects, and responds to security incidents in real-time.
- Rapid Response: Reduce the time between threat detection and response, minimising potential damage and ensuring swift recovery.

POTENTIAL CONSEQUENCES OF THE SECURITY COMPROMISE

It is unclear what data was accessed and potentially exfiltrated by the attackers. The LSSA is, however, confident that the unauthorised access:

1. has been restricted to a limited period; and
2. will not be repeated due to the introduction of additional control measures.

As stated above, we are unaware of any unlawful use of such personal information.

Specific personal information that may have been access:

1. Name, Surname, Identity Number
2. Contact details
3. Address details
4. Date of birth
5. Banking particulars
6. Demographic categorisation
7. Educational History

Please note: No biometric, access control, credit card, or personal sensitive information is being processed by the LSSA.

The authorised access was an attempt at demanding financial compensation to retain access to records. This has been restored without the LSSA having to make any payments to the unauthorised user.

We do not envisage that the consequences of the unauthorised access would have any of the following adverse consequences to you as a data subject:

1. Limiting your ability to access any services
2. Causing financial loss
3. Causing reputational loss
4. Causing loss of confidential information
5. Causing physical or psychological harm

WHAT CAN YOU DO TO MINIMISE THE POTENTIAL CONSEQUENCES OF THE SECURITY COMPROMISE

Potential adverse consequences of the security compromise may include:

1. increased phishing or spam emails.
2. attempts of identity fraud, e.g.: creation of fake social media accounts or fake applications at financial institutions; and
3. unsolicited direct marketing communication.

As stated in our Privacy Policy, the LSSA has taken reasonable measures to ensure the security and integrity of personal information being processed by us. Several measures have been introduced and reviewed by the LSSA recently, including control measures, policies and ongoing training.

WHAT MEASURES SHOULD YOU TAKE TO MITIGATE THE POSSIBLE ADVERSE EFFECTS?

We recommend that you take the following measures to mitigate potential adverse effects associated with the breach:

1. **Change Passwords**: Change the passwords for all online accounts, especially email, banking, and social media accounts. Make sure that the new passwords are strong and comply with industry recommendations.

2. **Introduce Multi-Factor Authentication**: Where possible, activate Multi-Factor Authentication for online accounts.

3. **Monitor Financial Statements**: Regularly review all bank statements for any suspicious or unauthorised transactions and immediately report any discrepancies to your financial institution.

4. Monitor credit application

5. **Update Security Software**: Ensure that your antivirus and anti-malware software is up-to-date on all your devices to protect against potential threats.

6. **Beware of Phishing**: Be alert of phishing attempts via email, text messages, or phone calls. Don't click on suspicious links or divulge personal information to unknown sources.

7. **Review Privacy Settings**: Review and update privacy settings on your social media profiles and other online accounts to limit the amount of personal information visible to the public.

DO WE KNOW WHO DID THIS?

We have received a letter from the State Security Agency on 11 October that the following was posted.

1. *ECS-CSIRT has detected a data leak published by the ALPHV ransomware group of data belonging to the Law Society of South Africa (LSSA).*

2. *2. The details of the leak are as follows: Timestamp: 2023-10-09T10:26:37+00:00 Provider: ALPHV Name: Law Society of South Africa*

We take the security of your personal information very seriously.

We sincerely apologise for the data breach and the inconvenience, trauma, and potential hazards this criminal activity has caused you.

We will monitor the situation and provide feedback at regular intervals.

Yours sincerely

Anthony Pillay
Executive Director
Law Society of South Africa
Tel: Switchboard: +27 (0)12 366 8800 ▪ Fax: +27 (0)86 677 8832
P O Box 36626, Menlo Park 0102 ▪ Docex 82, Pretoria
E-mail: tony@LSSA.org.za www.lssa.org.za