Impact Holdings (Pty) LTD trading as
IMPACT METER SERVICES
DIENSTE
REG. NO.: 2002/023813/07

Website: www.amps.co.za | Email: impact@amps.co.za | Tel: 012 763 8200

Date: 13/12/2022

To: **ALL DATA SUBJECTS OF IMPACT METER SERVICES**

NOTIFICATION OF A SECURITY COMPROMISE IN TERMS OF SECTION 22 OF PROTECTION OF PERSONAL INFORMATION ACT, 4 OF 2013 (POPIA)

1. In terms of Section 22 of POPIA, 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 the data subjects and the Information Regulator (Regulator), unless the identity of such data subject cannot be established.

2. It is in this respect that Impact Meter Services wishes to notify potentially affected persons who are data subjects of Impact Meter Services about the ransomware that has attacked the systems of Impact Meter Services on 22 November 2022.

3. Impact Meter Services have implemented security measures on all of its systems before such attack occurred. These measures include physical security of servers, surveillance, access control and includes the appointment of external IT consultants who have implemented measures such as firewall, monitoring, security response policy including regular backups, controlling of remote access, software development, anti-virus, user passwords, mail security, payment data security and monitoring of platform abuses.

4. We regret to advise that one of our service providers inadvertently omitted to update and run patches on the Impact Meter Services IT infrastructure which resulted in a breach of our systems by cyber criminals.

Brief description of the incident and the number of data subject(s) whose personal information has been compromised.

4.1. The security compromise took place on the evening of the 22nd of November 2022 wherein the systems of Impact Meter Services were encrypted and made unavailable to Impact Meter Services.

4.2. A ransom note was left by a Lockbit 3.0.

4.3. Impact Meter Services have employed the services of expert Cyber specialists who have ascertained that the hackers responsible for the ransomware have accessed and acquired Impact Meter's data held on its networks. We are writing to alert you of the possibility that some of your personal data *may* have been subject to unauthorized access and/or acquisition.

4.4. The attack was made by bypassing Impact Meter Services' firewall.

5. Data Subjects possibly affected:

Clients, service providers, suppliers and employees of Impact Meter Services.

6. Number of Data subjects

Not known

7. Types of personal data:

7.1. Names and Surname

7.2. Email address

7.3. Identity number

7.4. Physical address

7.5. Postal address

7.6. Contact numbers

7.7. Bank account number

8. Description of the possible consequences of the security compromise

The possible consequences are the selling of the personal information, identity theft, and fraud being committed should the personal information be used for those purposes.

9. Description of the measures that the responsible party intends to take or has taken to address the security compromise:

9.1. Impact Meter Services have appointed high end IT specialists to investigate the scope of the attack who will take, inter alia, the following steps:

Containment

Rapid Response & Threat Hunting

Log file processing and analysis

Eradication of malware/ ransomware within environment

Roll-out and Managed services on endpoint monitoring (SentinelOne EDR/ AV)

Threat Actor Intelligence Investigation

Support

9.2. Impact Meter Services and their Cyber Security consultants and IT consultants have successfully eradicated the ransomware/malware and all files have been subsequently decrypted. Our IT team are continuously working on the improvement of its security measures to ensure that such attack does not reoccur.

10. The identity of the unauthorised person who may have accessed or acquired the personal information.

The only identity known to the Responsible party is that the ransomware was conducted by Lockbit 3.0.

11. Advice or recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise.

11.1. Impact Meter Services advises that you:

11.1.1. remain vigilant by reviewing your account statements; and

11.1.2. immediately contact the law enforcement in the event of actual or suspected identity theft.

11.1.3. change your passwords as soon as possible and it is advisable to regularly change all passwords and security questions.

11.1.4. don't use the same password everywhere.

11.1.5. monitor your credit rating

11.1.6. watch your accounts, check your credit reports

11.1.7. do not disclose personal information such as passwords and PINS when asked to do so by anyone.

11.1.8. verify all requests for personal information and only provide it when there is a legitimate reason to do so.

12. For further assistance please contact us at: popia@amps.co.za

George Farmer

Managing Director

For and on behalf of Impact Meter Services