IMPORTANT NOTE

THIS IS A COPY OF THE NOTIFICATION MADE BY PAGEUP PEOPLE LIMITED TO THE OAIC ON 12 JUNE 2018.

A NUMBER OF EDITS HAVE BEEN MADE TO THIS DOCUMENT FOR OPERATIONAL SECURITY PURPOSES.

PLEASE ALSO VISIT THE PAGEUP SECURITY INCIDENT WEB SITE FOR MORE UP TO DATE INFORMATION ON THE BELOW INCIDENT

Melbourne
Sydney
Singapore
Hong Kong
Philippines
New York
London
pageuppeople.com

ABN 71 005 630 740

[redacted]
Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001
[redacted]

COPY TO:
[redacted]
Assistant Director
Office of the Australian Information Commission
[redacted]

12 June 2018
Matter 82667036
By Email

Dear [redacted]

PageUp People – Security Incident

Further to our conversations on 4th and 6th June 2018, and further to our letter of 8th June 2018, PageUp would like to notify the OAIC that it has reasonable grounds to believe that it has experienced an eligible data breach on 28th May 2018. We have set out the details of the data breach below and have provided as much information as we can confirm at this time. This is largely an update on the information that we provided in our letter of 8 June.

1 Organisation details

Organisation name:	PageUp People Limited
Address:	**Australia**:

Level 10, 91 William Street, Melbourne, 3000, Australia

UK:

71-75 Shelton Street Garden Studios, Covent Garden, London, WC2H 9JQ

Contact person: [redacted]

Email: [redacted]

Data protection office: [redacted]

Phone: [redacted]

Email: [redacted]

---

2 Description of the data breach

Data breach descriptin

- A vulnerability in PageUp's Australian web infrastructure was exploited on or around 15th May 2018, by an unknown threat actor. This activity was caused by malware that had not been detected by our anti-malware vendor
- On 23rd May 2018, PageUp became aware of unusual activity affecting its IT infrastructure and initiated its ISO 27001 security incident response plan. We established evidence of malware that was not detected by our anti-malware vendor, which was likely used to establish a foothold on the network and achieve unauthorised remote access
- We worked to establish containment and eradication, whilst launching a forensic investigation to establish what, if any, data may have been accessed or exfiltrated.
- At the time of our letter of 8 June, our analysis had identified unauthorised queries of our databases, however at that stage it was not possible to ascertain with absolute certainly what, if any, data had been accessed. If personal data had been compromised, potential impact would have included unauthorised access or loss of personal data or hashed and salted passwords. But at that point we were not aware of any actual harm to any individuals.
- As at the time of this letter, further forensic work has been completed and we believe that we now have additional evidence of what has been accessed and whilst we have no direct evidence of exfiltration we believe that, given the possibility of "serious harm" occurring based on the data accessed we believe that an eligible breach may have occurred.

Date the breach occurred

We believe that a vulnerability in PageUp's Australian web infrastructure was exploited on or around 15th May 2018, by a criminal threat actor, facilitating unauthorised remote access.

Date the breach was discovered	On 23rd May 2018, PageUp People became aware of unusual activity affecting its IT infrastructure. On 28th May 2018, further analysis identified unauthorised access had occurred between 15th May and 23rd May.
Primary cause of the data breach	Threat actor, who exploited a vulnerability in a web server using malware to obtain unauthorised remote access.
No. of individuals with Personal Information affected	The number of personal data records concerned depends on the queries run by the unauthorised party and which databases were accessed. Work is ongoing to ascertain, to the extent it can be determined, the volume of records and contents returned by those. We are working with forensic consultants to analyse the unauthorised access to our database infrastructure with a view to determining what personal data may have been accessed and this work is ongoing.
Categories of individuals affected	• Employees of PageUp and PageUp's clients • Job applicants for PageUp and PageUp's clients
Investigation and assessment steps taken	(1) 23rd May 2018 • PageUp became aware of unusual activity affecting its IT infrastructure and immediately enacted our ISO 27001 incident response plan. (2) 24th May 2018 • PageUp engaged an independent third-party organisation to commence a digital forensics investigation. (3) 24th to 25th of May 2018 • Containment and verification that the threat had been eradicated. (4) 26th May 2018 • PageUp worked with our anti-malware vendor to enable them to update their protection to prevent further exploits using the same malware. (5) 28th May 2018 • PageUp identified access to database servers in our UK data centre, prior to 24th May, and subsequently identified similar activity on our database servers in the Australian data centre. (6) 6th June 2018 • Confirmed that there is no evidence that the document storage infrastructure had been compromised. (7) 7th June 2018 • Since 28th May, we have been analysing evidence, in conjunction with our independent forensics partner and have not yet been able to confirm with certainty what data may have been accessed, or if any data may have been exfiltrated, although investigations are continuing.

(8) 9th – 12th of June

- Since our previous letter of 8th of June forensic work has continued by both our IT team and third party experts and we have been able to identify with greater clarity the data that has been accessed. We have not yet ascertained definite proof of exfiltration but there is a reasonable probability that this has occurred. Work continues in this area.

Remedial action taken to assist individuals

(1) 1st June 2018

- PageUp's Australian clients were notified of the incident.

(2) 2nd June 2018

- PageUp issued a daily update to Australian clients notified of the incident.

(3) 3rd June 2018

- PageUp issued a daily update to Australian clients notified of the incident.

(4) 4th June 2018

- PageUp issued a daily update to Australian clients notified of the incident

(5) 5th June 2018

- PageUp issued a daily update to Australian clients notified of the incident

(6) 6th June 2018

- PageUp held a national event for impacted Australian clients, in conjunction with the Joint Cyber Security Centre (JCSC) and the Australian Computer Emergency Response Team (CERT).

(7) 7th June 2018

- PageUp held a national event for impacted Australian clients, in conjunction with the Joint Cyber Security Centre (JCSC) and the Australian Computer Emergency Response Team (CERT).

(8) 12th June

- PageUp will be providing comprehensive communications to our clients in conjunction with this filing and will be working with our customers to assist them in communicating with impacted individuals
- PageUp will work with its employees and candidates to ensue that they are communicated with in a timely manner
- PageUp will make public statements and update its website to ensure information about the breach is available

Additionally, PageUp have been supporting its clients to reset account passwords.

Action taken / intending to take

- [Note – omitted due to operational security]

---

to prevent reoccurrence	
Notification to clients who may have been affected	See communications notifying individuals at Schedules 1 to 8 of this letter. (1) 29th May 2018 • Impacted UK clients were notified by email at 07:01am AEST (10:01 UK time). (2) 1st June 2018 • Additional communications sent to UK clients by email, using "super user" accounts. • Communications were sent to Australian clients by email at 17:31 AEST. (3) 2nd June 2018 • All Australian and UK clients were notified by email at 17:58 AEST. (4) 3rd June 2018 • Additional communications sent to Australian and UK clients by email at 16:23 AEST. (5) 4th June 2018 • Additional communications sent to Australian and UK clients by email at 17:49 AEST. (6) 5th June 2018 • At 18:34 AEST PageUp published the security incident advisory on www.pageuppeople.com to inform all clients of the incident status. • Additional communications sent to Australian and UK clients by email at 18:56 AEST, referencing the published the security incident advisory. (7) 6th June 2018 • 14:00 AEST PageUp hosted a national event for impacted Australian clients, in conjunction with the Joint Cyber Security Centre (JCSC) and the Australian Computer Emergency Response Team (CERT), which a number of our affected clients attended. (8) 7th June 2018 • 15:00 AEST PageUp hosted a national event for impacted Australian clients, in conjunction with the Joint Cyber Security Centre (JCSC) and the Australian Computer Emergency Response Team (CERT), which a number of our affected clients attended. (9) 12th June 2018 • Communication to clients notifying them that there has been an eligible data breach.
Other bodies / authorities notified	**Australia:**

- Australian Cyber Security Centre (**ACSC**), via web submission on 1st June 2018
- Australian Computer Emergency Response Team (**CERT**) made contact with PageUp on 1st June 2018
- The Office of the Australian Information Commissioner (**OAIC**) were initially notified of the incident on 4th June 2018.
- The Australian Federal Police

UK:

- Information Commissioner's Office (**ICO**) submitted on 1st June 2018

Additional information	The anti-malware software we were running was up to date as at the date of the incident.

3 Type of information involved in the data breach

The impacted infrastructure includes applicant and user data that our clients configured for their environment, including application forms that include applicant names and anything our clients' recruiters or users had configured for use within the "Recruitment" modules of the solution. The resumes and documents uploaded are not stored on the impacted infrastructure.

General

We are confident that the most critical sensitive information categories including resumes, financial information, employee performance reports, Australian tax file numbers and employment contracts are not affected in this data breach.

Some general corporate account password data may be affected for assessment providers, FTP exports, and in a very limited number of cases, service accounts. While these are also stored in a format that cannot be reused, as a precaution we have reset the passwords that we store for these purposes and have been in contact with all clients to reset the credentials on their end. Links to external systems and associated credentials were also accessed but were in a format that cannot be reused.

Some personal data for employees who currently or previously had access to the client's PageUp instance may also be affected. This includes employee contact information (including name, email address, physical address, and telephone number) and employment information (including employment status, company and title, and whether they were the registered contact for communications from PageUp). For those employees who currently or previously had access to the client's PageUp instance, current password data is in a format that cannot be reused and therefore is considered to be of very low risk to individuals. However, failed login attempt data from 2007 and before contained some password data in clear text. If employees have not changed their password information since 2007, it would be prudent to do this now and anywhere where they have used the same password.

Applicants

The following information for applicants may also have been affected:

- contact details including name, email address, physical address, and telephone number;
- biographical details including gender, date of birth, and maiden name (if applicable), nationality, and whether the applicant was a local resident at the time of the application; and
- employment details at the time of the application, including employment status, company and title. If the application was submitted for a reference check, then the following additional details may have been provided by the reference: technical skills, special skills, team size, length of tenure with company, reason for leaving that position (if applicable), and the length of relationship between the applicant and reference

Password data for applicants is in a format that cannot be reused and therefore believed to be of very low risk to these individuals.

References

For references who were included with an applicant's information, contact information (including name, email address, physical address, and telephone number) and employment information at the time the reference was provided (including company, title, and the length of the relationship with the applicant) are affected.

4 Steps recommended to individuals

We are recommending that individuals take the following steps

(a) change their passwords on other online services, if they re-use the same password;

(b) enable multi-factor authentication and other available security measures provided by their other online services;

(c) be aware of potential phishing emails and telephone calls from businesses or institutions requesting their personal details, or other suspicious or fraudulent activity. We are giving examples such as they might receive communications pretending to be from previous employers, or from other companies offering fictitious employment roles, or other scams seeking to elicit their payment/banking details or other personal information, or otherwise seeking to defraud them. We are recommending they are vigilant at all times;

(d) avoid opening attachments from unknown senders via email or social media;

(e) install anti-virus software and keep it updated; and

(f) apply all recommended software patches from operating system and software providers.

Yours sincerely

Karen Cariss

CEO