Office of the Information and Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Anglo American Services (UK) Limited (Organization)
Decision number (file number)	P2019-ND-005 (File #009035)
Date notice received by OIPC	June 28, 2018
Date Organization last provided information	July 3, 2018
Date of decision	January 3, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported: *At this stage it has not been possible to determine with certainty what personal data of Albertans may have been accessed, but we understand … that the breach could extend to the following information relating to data subjects:* *- employment details such as employment status, company and title;* *- biographical information including gender, date of birth, maiden name, nationality, residency;* *- identification data such as identity number, national identification number, social security number, ID numbers (but according to our subsequent investigations, we are not aware that such data relating to [the Organization's] data subjects was accessed);* *- details provided by data subjects' references (e.g. technical skills, special skills, team size, length of tenure with company, reason for leaving that position, length of relationship between the applicant and reference);* *- some usernames and passwords may have been accessed.*

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• PageUp People Ltd. (PageUp) provides recruitment support services to the Organization and acts as the Organization's data processor. PageUp provides a hosted platform through which candidates view and apply for job vacancies in the Organization. • On June 6, 2018, the Organization became aware (via a press article) of a security incident affecting the PageUp platform. • On June 12, 2018, PageUp confirmed that the incident involved a cyberattack to gain unauthorized access to PageUp's IT systems in Australia, Singapore and the UK. PageUp also confirmed that the threat was contained and eradicated. • The Organization said that according to PageUp, the incident occurred on May 15, 2018.
Affected individuals	The incident affected approximately 11,525 individuals based in Alberta.
Steps taken to reduce risk of harm to individuals	• Suspended the PageUp application portal preventing any new applicant data from being introduced. • Set-up work arounds to enable job applicants to continue applying for vacancies without using the PageUp portal. • Reset all users' passwords (done by PageUp). • Liaised with PageUp to review the controls currently in place and resolutions that were put in place. • Identified any element of potentially compromised information being exposed externally. • Posted a notice about the incident on its website. • Notified the Organization's personnel.
Steps taken to notify individuals of the incident	Affected individuals were notified by email between June 25 and June 28, 2018.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with	The Organization reported: *According to PageUp, at this stage it is not possible to determine with certainty what harm may have been caused to Alberta data subjects, as there is no evidence that personal data which may have been accessed has been used adversely. However, given the nature of the personal data*

non-trivial consequences or effects.	*involved, there is a potential risk that the breach could lead to data subjects suffering:* - *loss of control over their personal data/damage to reputation* - *identity theft or fraud* - *financial loss (through identity theft or fraud)* The Organization also said "Depending on the personal information accessed (e.g. employee reference information), this could lead to reputational harm for some individuals." In my view, a reasonable person would consider that the comprehensive identity and employment information at issue could be used to cause the harms of identity theft, fraud and financial loss. Reference information could be used to cause reputational damage, embarrassment or humiliation. Credentials could be used to compromise other online accounts. These are all significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	In assessing the likelihood that harm would result from this incident, the Organization reported it is "not possible to determine at this time…". In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and installation of malware). It is not clear from the Organization's report how long the information may have been exposed.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.

A reasonable person would consider that the comprehensive identity and employment information at issue could be used to cause the harms of identity theft, fraud and financial loss. Reference information could be used to cause reputational damage, embarrassment or humiliation. Credentials could be used to compromise other online accounts. These are all significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and installation of malware). It is not clear from the Organization's report how long the information may have been exposed.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by email between June 25 and June 28, 2018, accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner