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	Orica Australia Pty Ltd. (Organization)
Decision number (file number)	P2018-ND-078 (File #008999)
Date notice received by OIPC	June 21, 2018
Date Organization last provided information	July 3, 2018
Date of decision	July 16, 2018
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
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"	Information involved in the incident was provided by job applicants using PageUp, a third party, cloud-hosted system that the Organization uses for online recruitment. The Organization reported the following application fields may have been accessed: • name, • title, • date of birth, • date created, • date last edited, • gender, • home country, • home telephone number, • home state/territory, • home street, • home suburb, • internal/external, • last activity date, • mobile number, • nationality, • nominated employment status,

	• person ID, • phone 3, • postcode, • preferred name, • source and sub source, • total number of applications, • language country, • country of origin, • residency, • visa expiry, • visa number, • visa type, • current salary, • expected salary, • currency, • driver's license number, • social insurance number, • banking information, • occupational license, and • referee contact information. 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, I have jurisdiction in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On June 1, 2018, PageUp, a third party, cloud-hosted system that the Organization uses for online recruitment, sent its customers a generic email advising that PageUp detected unauthorized activity in its system on or around May 23, 2018. • The email provided all users with notice that an investigation was occurring but did not specifically indicate that any information relating to the Organization was accessed or otherwise compromised. • On June 12, 2018, PageUp issued a statement that "We believe certain personal data relating to our clients, placement agencies, applicants, references, and our employees has been accessed." • The Organization reported "The suspected cause of the breach (as stated by Page Up) is that malware initiated the intrusion" and that the unauthorized activity was detected by PageUp in their system on or around May 23, 2018; however "…the possibility that the intrusion occurred earlier remains…".

Affected individuals	The Organization cannot determine the number of Alberta residents affected by the breach but knows that since 2004, 2,196 residents of Alberta used PageUp to provide the Organization with a job application.
Steps taken to reduce risk of harm to individuals	• Requested additional information from PageUp. • Stopped active advertising of jobs through the PageUp portal. • Asked PageUp to force password resets for all applicants for positions with the Organization and related entities. • Requested that more individuals at the Organization be informed of the progress being made by PageUp. • Published a notice on the Organization's external website and issued it to existing employees. • Requested that individuals change their login details. • Referred individuals to the Office of the Australian Information Commissioner and PageUp for more information.
Steps taken to notify individuals of the incident	• The Organization said it was currently taking steps to determine the contact details of Alberta residents who may have been affected by the breach. The Organization stated that "to the extent we can track down contact information of Alberta residents who have used PageUp to apply for positions in the Organization, we will be sending them notification." • The Organization posted a notification on its website and provided communications to its employees.
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 non-trivial consequences or effects.	The Organization reported that "It is not possible to properly assess the potential impact without specific detail on what personal information was accessed as a result of the unauthorized activity in PageUp's system. PageUp has not yet supplied the information and [the Organization] is not aware of any actual harm to data subjects." In my view, the comprehensive information at issue – including contact, identity, employment and financial information – could be used to cause the significant harms of identity theft, fraud and financial loss.
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.	The Organization reported that it "…is not currently in the position to determine whether or not there could be significant consequences as a result of the breach. Nonetheless, To the extent [the Organization] is able to obtain contact information for any of the 2196…applicants in Alberta who have used the PageUp system since 2004, [the Organization] will notify the individuals as a precautionary measure to assist the individual in taking protective steps."

	In my view, 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). Further, the Organization does not know how long the information was 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.

The comprehensive information at issue – including contact, identity, employment and financial information – could be used to cause the significant harms of identity theft, fraud and financial loss. 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). Further, the Organization does not know how long the information was exposed.

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

Section 19.1(1) of the Regulation states "Where an organization is required under section 37.1 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must …be given directly to the individual". However, pursuant to section 19.1 (2), "…where an organization is required to notify an individual under section 37.1 of the Act, the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

In this case, the Organization reported that it "…is not currently in the position to determine whether or not there could be significant consequences as a result of the breach. Nonetheless, to the extent [the Organization] is able to obtain contact information for any of the 2196…applicants in Alberta who have used the PageUp system since 2004, [the Organization] will notify the individuals as a precautionary measure to assist the individual in taking protective steps."

Given this, and pursuant to section 37.1(2) of PIPA which states "… the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate…", **I require the Organization to report to my office within ten (10) days of the date of this decision, that affected individuals have been notified of this incident directly in accordance with the requirements outlined in the Regulation, or, why the Organization believes that direct notification is unreasonable and how it intends to notify affected individuals indirectly.**

Jill Clayton
Information and Privacy Commissioner