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	AltaLink Management Ltd. o/b/o AltaLink Limited Partnership (Organization)
Decision number (file number)	P2023-ND-010 (File #027470)
Date notice received by OIPC	September 22, 2022
Date Organization last provided information	December 1, 2022
Date of decision	February 3, 2023
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 whose personal information was collected in Alberta pursuant to section 37.1 of *the Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is headquartered in Calgary and is an "organization" as defined in section 1(1)(i) of PIPA.

Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information:
	
	• name,
	• home address,
	• email address,
	• telephone number,
	• resumes, including:
	  ○ work experience,
	  ○ educational background,
	  ○ education results including test scores,
	  ○ scholarships,
	  ○ professional designation,
	  ○ personal interests,
	  ○ familial circumstances, and
	• comments made during recruitment processes.
	
	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• At the time of the incident, the Organization obtained cloud-based recruitment services provided by a third party vendor (HireGround). • On September 7, 2022, the Organization's vendor was victim to a cyberattack. The threat actor subsequently "gained access to the database back-up" and obtained personal information. • The incident was discovered on or about September 19, 2022, when the Organization received demands for financial compensation in exchange for destroying "stolen documents/data."
Affected individuals	The incident affected approximately 10,000 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• The third party vendor deleted the abused accounts. • "Removed the link to the job application environment from [the Organization's] website." • Reviewing security of cloud based applications provided by third parties.
Steps taken to notify individuals of the incident	The Organization's third party service provider notified affected individuals by email on September 22, 2022.
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 the possible harms of: *- increased vulnerability to identity theft and fraud* *- increased vulnerability to phishing* *- potential embarrassment* I agree with the Organization's assessment. A reasonable person would consider the contact information (name, home address, email address, telephone number), resumes containing biographical details (work experience, education, designations, interests, etc), and comments made during the recruitment process could be used to cause the harms of identity theft, fraud, embarrassment, and possibly loss of business or professional opportunities. Email addresses could be used for the purposes of phishing, increasing affected individuals' vulnerability to the above. These are 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.	The Organization did not provide an assessment on the likelihood that significant harm will result. They reported: *Assessment of likelihood of harm is unknown at this time. [The Organization] has knowledge that the cybercriminals have obtained documents/ data from the third-party vendor system. [The Organization] has now been informed that the cyber-criminals are known to have previously conducted similar incidents and released similar information publically.* In a December 1, 2022 update, the Organization reported: *At this time we are unaware of any use or release of any information which was accessed (resumes) and unaware of any harm as a result of this compromise.* *[The Organization] has been advised by … (company specializing in analysis of threat intelligence information) that the cyber criminals involved in this breach do not routinely engage in ransomware compromises or resell the exfiltrated data on the dark web. Rather their motivation is one of enhancing their reputation among their peers for the numbers of systems and accounts that have been breached.* *Furthermore, [the Organization] routinely monitors the dark web forums for any traffic associated with our corporate systems and networks, and have not detected any harmful activity associated with this unauthorized access.* 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 a threat actor (deliberate intrusion, exfiltration of records, and extortion). The Organization confirmed personal information was exfiltrated; a lack of evidence that the personal information has been misused does not mitigate against future harm as identity theft and fraud can occur months or years after a breach.

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 the contact information (name, home address, email address, telephone number), resumes containing biographical details (work experience, education, designations, interests, etc), and comments made during the recruitment process could be used to cause the harms of identity theft, fraud, embarrassment, and possibly loss of business or professional opportunities. Email addresses could be used for the purposes of phishing, increasing affected individuals' vulnerability to the above. These are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a threat actor (deliberate intrusion, exfiltration of records, and extortion). The Organization confirmed personal information was exfiltrated; a lack of evidence that the personal information has been misused does not mitigate against future harm as identity theft and fraud can occur months or years after a breach.

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's third party service provider notified affected individuals by email on September 22, 2022 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance