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	Advocate Sherman Hospital (Organization)
Decision number (file number)	P2019-ND-069 (File #011719)
Date notice received by OIPC	January 16, 2019
Date Organization last provided information	January 16, 2019
Date of decision	May 31, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individual 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 operates in Elgin, Illinois, 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: • first and last name, • address, • email address, • telephone number, and • other information included in a resume (e,g, educational background and work experience). 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 in this case.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• In October 2018, the Organization received a letter from Bullhorn, Inc.'s Jobscience, one of the Organization's former job application management and employee onboarding service providers, notifying the Organization of an incident.

	• The Organization understands from Jobscience that on or around May 8, 2018, an unauthorized third party gained access to data contained on Jobscience's server used to process employee application information and exfiltrated the database of one of Jobscience's service applications. • Jobscience learned about the attack from the FBI in late August. • Jobscience confirmed to the Organization in November 2018 that one Alberta resident was affected. The information at issue is from a resume that predates 2013.
Affected individuals	The incident affected 1 Alberta resident.
Steps taken to reduce risk of harm to individuals	• The Organization no longer has an ongoing business relationship with Jobscience. • Jobscience has committed to the Organization that it has remedied the underlying cause of the unauthorized access, forced a password reset for all active accounts, and taken steps to implement additional security controls.
Steps taken to notify individuals of the incident	The affected individual in Alberta was sent a written notification by mail on December 13, 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 non-trivial consequences or effects.	The Organization did not specifically identify any harm(s) that might result from this incident, but its notification to the affected individual in Alberta said: *While Jobscience has no evidence to indicate that your information has or will be used inappropriately, it is always a good idea to protect your personal information by following strong password practices, using random passwords, and creating a different password for every website.* *Additionally, you should exercise caution when responding to unsolicited emails requesting your personal information or account credentials, or emails that link you to a website that requests you to enter personal information or account credentials.* In my view, a reasonable person would consider that the contact and employment information at issue could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to identity theft and harm.

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 as assessment of the likelihood of harm resulting from this incident but reported there is "…no evidence of misuse of the personal information in question." In my view, the likelihood of harm resulting from this incident is increased because the incident was the result of malicious intent (deliberate unauthorized intrusion and exfiltration). The information was apparently exposed for over four months. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing or identity theft and fraud can occur months and years after a data 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 that the contact and employment information at issue could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to identity theft and harm. The likelihood of harm resulting from this incident is increased because the incident was the result of malicious intent (deliberate unauthorized intrusion and exfiltration). The information was apparently exposed for over four months. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing or identity theft and fraud can occur months and years after a data breach.

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

I understand the affected individual in Alberta was sent a written notification by mail on December 13, 2018. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner