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	Canadian Back Institute Operating Limited Partnership (Organization)
Decision number (file number)	P2020-ND-152 (File #015904)
Date notice received by OIPC	May 12, 2020
Date Organization last provided information	May 12, 2020
Date of decision	November 20, 2020
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 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 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: • employee name, • address, • date of birth, • Social Insurance Number, • personal telephone number, • personal email address, and • banking 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, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• An Ontario payroll administrator's password was compromised, resulting in unauthorized access to a cloud-based employee payroll system.

	• During the unauthorized access, banking information was changed for a subset of seven (7) employees (one (1) in Alberta). • The breach occurred between approximately March 29, 2020 and April 15, 2020. • The Organization learned of the breach on April 15, 2020 when an unauthorized change to banking information was discovered, and an investigation was commenced.
Affected individuals	The incident affected 224 individuals, including 18 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Providing credit monitoring and identity theft insurance for affected individuals. • Notified employees whose banking information was changed. • Reset password for the compromised account. • Accelerated roll out of multi-factor authentication to access the cloud-based payroll system. • Changed procedure for processing direct deposit change requests. • Rollout of advanced employee security training.
Steps taken to notify individuals of the incident	Employees who had banking information changed were notified by telephone on or about April 18, 2020, and all affected individuals in writing on or about April 27 - 28, 2020.
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 Commissioner has previously concluded in cases such as Children's Wish Foundation of Canada P2019-ND-182 that unauthorized access to financial and employment information could be used to cause the harms of identity theft and fraud.* In addition, the Organization's notification to affected individuals, provided an information sheet for credit monitoring services and advised individuals how to protect themselves from phishing emails and text messages. In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. 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.	The Organization reported "In this case, the fact that there is actual evidence of malicious changes to banking information for a subset of individuals (1 in Alberta) increases the risk of harm". In my view, a reasonable person would consider 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). In this case, there is actual evidence of malicious activities. Further, the information may have been exposed for approximately two (2) weeks.

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, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. 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). In this case, there is actual evidence of malicious activities. Further, the information may have been exposed for approximately two (2) weeks.

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

I understand the Organization notified individuals whose banking information was changed by telephone on or about April 18, 2020, and all affected individuals were notified in writing, on or about April 27 - 28, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner