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 Physiotherapy Association (Organization)
Decision number (file number)	P2020-ND-048 (File #015671)
Date notice received by OIPC	April 8, 2020
Date Organization last provided information	April 8, 2020
Date of decision	May 19, 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 the following information: • name, • email address, • contact information, • social insurance number. The 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	• On October 24, 2019, the Organization learned that it was the victim of a social engineering and phishing attack when a vendor followed up regarding payment of an invoice.

	• The Organization discovered a wire transfer had been made to a threat actor posing as the vendor. • On November 21, 2019, following an investigation, the Organization learned that there had been an intrusion into two employee inboxes. The suspected point of entry was a phishing email likely received by the employees. • The Organization reported it is possible that the threat actors exfiltrated the contents of one of the inboxes, although there is no evidence indicating the threat actor has misused any of the personal information to which it may have access. • The incident occurred between October 2, 2019 and November 26, 2019.
Affected individuals	The incident affected 348 individuals, including 21 in Alberta.
Steps taken to reduce risk of harm to individuals	• Ensured employees and staff reset passwords. • Blocked all suspected fraudulent domain addresses; • Reported the incident to the RCMP Canadian Anti-Fraud Centre on November 12, 2019 as well as privacy regulators. • Emailed staff and membership to be vigilant when using email, and provided risk management strategies to prevent further cyber attacks. • Implemented multi-factor authentication and arranging for mandatory cybersecurity and privacy training for staff. • Arranged for a call center with a designated toll free number that affected individuals can call for information. • Provided affected individuals, whose social insurance number and credit card information was implicated, with 1 year of complimentary credit monitoring and identity theft insurance.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone and email between April 6, 2020 and April 13, 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 it has "…determined that there is a real risk of significant harm to the affected individuals (ie. the risk of financial harm, identity theft and phishing) based on the possibility that one of the lnboxes may have been exfiltrated by the threat actor". In my view, a reasonable person would consider that the contact and identity information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud.

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.	As noted above, the Organization reported it has "…determined that there is a real risk of significant harm to the affected individuals … based on the possibility that one of the lnboxes may have been exfiltrated by the threat actor". In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach resulted from malicious intent (deliberate, phishing, fraudulent representation) and the information may have been exfiltrated. The incident occurred over the course of almost 2 months.

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 identity information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud.

The likelihood of harm resulting from this incident is increased as the breach resulted from malicious intent (deliberate, phishing, fraudulent representation) and the information may have been exfiltrated. The incident occurred over the course of almost 2 months.

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 affected individuals were notified by telephone and email between April 6, 2020 and April 13, 2020. The Organization is not required to notify the individuals again.

Jill Clayton
Information and Privacy Commissioner