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	Alberta College and Association of Opticians (the "Organization")
Decision number (file number)	P2019-ND-124 (File #011616)
Date notice received by OIPC	January 11, 2019
Date Organization last provided information	January 14, 2019
Date of decision	August 2, 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 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 reported that it is incorporated under Alberta's *Societies Act*. It therefore qualifies as a "non-profit organization" as defined in section 56(1)(b)(i) of PIPA. Pursuant to section 56(2), PIPA "does not apply to a non-profit organization or any personal information that is in the custody of or under the control of a non-profit organization", except in the case of personal information that is collected, used or disclosed in connection with any commercial activity. In this case, the Organization is the regulatory body for opticians in Alberta. The Organization ensures licensure to practice as mandated by the *Health Profession Act* and collects all business and personal information for members along with licensing fees and fees for various courses/seminars. To the extent the personal information at issue in this case was collected, used or disclosed in connection with the Organization's commercial activities, PIPA applies.

Section 1(1)(k) of PIPA "personal information"	The Organization reported the incident affected email mailboxes and the Organization's database which contains: • email addresses, • addresses, • telephone numbers and work addresses. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On December 18, 2018, the Organization's server and system was hacked and infected with ransomware. • The breach was discovered the same day.
Affected individuals	The incident affected 2,000 individuals.
Steps taken to reduce risk of harm to individuals	• Server and data were restored from backups and then virus scanned. • Reviewed all security systems. • Changed all server/network administrative passwords. • Disabled remote desktop connections. • Reported to law enforcement. • Posted a server down notice on the website and Facebook, and included information in January e-newsletter.
Steps taken to notify individuals of the incident	All active members were notified by email sent January 10, 2019.
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 that could result from the breach are "Primarily ransom / extortion" and "… possibly damage to reputation / identity theft". Based on the Organization's report of the information at issue (email addresses, addresses, telephone numbers and work addresses), possible harms that might result from this breach include phishing, increasing vulnerability of affected individuals to identity theft and fraud. This is a significant 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.	With respect to assessing the likelihood of harm resulting in this case, the Organization reported "Still under investigation". In my view, given the limited information provided by the Organization, 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 an unknown third party (ransomware).

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.

Based on the Organization's report of the information at issue (email addresses, addresses, telephone numbers and work addresses), possible harms that might result from this breach include phishing, increasing vulnerability of affected individuals to identity theft and fraud. This is a significant harm.

Given the limited information provided by the Organization, 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 an unknown third party (ransomware).

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 all active members were notified by email sent January 10, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner