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 (Organization)
Decision number (file number)	P2020-ND-136 (File #014841)
Date notice received by OIPC	January 31, 2020
Date Organization last provided information	January 31, 2020
Date of decision	November 3, 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 those individuals 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 "…the regulatory body for Opticians in Alberta. We ensure licensure to practice as mandated by the Health Profession Act. We send emails to registrants, including mass e-mails when necessary." The Organization 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.
Section 1(1)(k) of PIPA "personal information"	The incident involved email addresses. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information at issue in this matter was collected, used or disclosed in connection with a commercial activity, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 30, 2020, an email was sent from a disused email account to an unknown number of people asking for a "favor" and for people to respond to the email. Most of the recipients are registrants of the Organization; some are vendors or other business contacts, some are staff members. • The Organization's IT technician quickly recovered the account and found that emails were being rerouted to a hotmail account. The hacker(s) had access to the account for approximately 10 – 15 minutes. • The breach was discovered on January 30, 2020 when staff members and the IT technician all received an email from the inactive account.
Affected individuals	The incident affected approximately 1,000 – 1,300 individuals.
Steps taken to reduce risk of harm to individuals	• Sent a mass email to alert people to the phishing email. • Answered phone calls and emails from people checking to see if it was a legitimate email. • Deactivated the retired account. • Deleted all inactive email accounts of previous employees. • All active email accounts have had password changes of increased length. • Posted a notice on Facebook and the Organization's website.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on January 30, 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 "This appears to have been a phishing scam. The initial email asked people to initiate further contact, and does not appear to have had any viruses attached to it, however if anyone contacted them during the small window when we did not have control, they could be opening themselves up to potential viruses sent back to them or further phishing scams." I agree with the Organization's assessment. A reasonable person would consider the information at issue could be used for phishing purposes, increasing vulnerability to identity theft and fraud. 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 reported that "Given the time of day (early morning), the nature of the initial email (asking for "a favor" and further contact, but not offering any malicious attachments), and the length of time we did not have access to the account (10-15 minutes) we believe the likelihood of harm is minimal. The email account that was accessed existed for less than 1 year and did not deal with extremely sensitive information, but was used once to send a mass email to all registrants which we believe is the reason so many people may have been affected." In my view, a reasonable person would consider that the risk of significant harm is increased as the breach resulted from malicious intent. The nature of the email and quick response from the Organization reduce the likelihood of significant harm; however, it is possible the perpetrator continues to have the list of email addresses, such that the information could be used for future phishing attacks.

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 information at issue could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.

The risk of harm is increased as the breach resulted from malicious intent. The nature of the email and quick response from the Organization reduce the likelihood of significant harm; however, it is possible the perpetrator continues to have the list of email addresses, such that the information could be used for future phishing attacks.

The Organization is required to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand that affected individuals were notified by email on January 30, 2020. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner