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)	P2021-ND-048 (File #010326)
Date notice received by OIPC	November 20, 2018
Date Organization last provided information	February 4, 2019
Date of decision	March 2, 2021
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 collect all business and personal information for our members along with licesning [sic] fees and fees for various courses/seminars". 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 all or some of the following information: • name, • email address, • billing address, • telephone number, • customer IP address, • type of credit card, last 4 digits of credit card number, expiry date, and

	• whether or not the purchase was approved. 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 November 9, 2018, the Organization's WordPress site was hacked. • The breach was discovered on November 12, 2018 by staff attempting to access the website who were redirected to a malicious ad-rich site. • The unauthorized users granted themselves administration accounts on November 10, 13 and 15, 2018. As such, they would have been able to see the personal information of individuals who paid for continuing education courses or employment ad space, and those who filled out ad forms. • On November 16, 2018, the website was fully cleaned and restored.
Affected individuals	The incident affected approximately 50 individuals.
Steps taken to reduce risk of harm to individuals	• Notified members to proactively improve their security. • Forced a password change on the continuing education website and encouraged members to change their passwords on their secure online profile. • Took the WordPress website down and cleaned it, and removed fake administration accounts, as well as inactive user accounts. • Restored settings to disallow self-account creation. • Changed administration passwords in several places. • Set up a maintenance schedule to ensure plugins and themes are maintained. • Update plugins and improved security for the continuing education website. • Will be removing forms and limiting the number of people whose billing information is stored on the website. • Providing extra security on the server so it can be quickly isolated if an event like this happens again.

Steps taken to notify individuals of the incident	Affected individuals were notified on November 13, November 19 and November 20, 2018 by email, e-newsletter and via the Organization's website.
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 affected individuals … *…may receive spam e-mails or scammer phone calls, or someone who knows their address might try to contact them. With their billing information, scammers might try to intimidate them into paying for something they didn't purchase, and the partial information could be used to try to extract more sensitive information from them. If their credit card information was somehow accessed, it could potentially be dangerous to them financially, however, as I understand it, the precautions we've taken to ensure that credit card information is entered in a secure payment gateway mitigates the risk of exposure.* In my view, a reasonable person would consider that the individual's contact information (name and address) could be used to send unsolicited mail, but I have not typically found this to be a significant harm. The financial information (the type of credit card, last four digits of a credit card and expiry date) is insufficient to be used for criminal purposes such as identity theft or fraud. Email addresses, however, could be used for the purposes of phishing, 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: *Given the nature of the attack (redirecting our website to ad-rich content) the end goal seems to have been ad revenue rather than theft of personal information. Because of the secure payment portal, the risk of credit card information getting out seems to be very low; the only exposed information is the billing information, which seems harder to use maliciously, but if the attackers gathered that information, they could potentially use it or sell it to someone who would for scamming purposes.* In my view, a reasonable person would consider the likelihood of harm resulting from this incident to be increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and the creation of fake administrators). The Organization can only

	speculate about the motivations of the attackers. Further, the information may have been exposed for eight days.

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 individual's contact information (name and address) could be used to send unsolicited mail, but I have not typically found this to be a significant harm. The financial information (the type of credit card, last four digits of a credit card and expiry date) is insufficient to be used for criminal purposes such as identity theft or fraud.

Email addresses, however, could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident to be increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and the creation of fake administrators). The Organization can only speculate about the motivations of the attackers. Further, the information may have been exposed for eight days.

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 the Organization notified affected individuals by email, e-newsletter and via its website on November 13, November 19 and November 20, 2018, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner