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 Medical Association (Organization)
Decision number (file number)	P2019-ND-130 (File #007148)
Date notice received by OIPC	November 23, 2017
Date Organization last provided information	July 19, 2018
Date of decision	August 9, 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 the individuals 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)(i) of PIPA. The Organization is incorporated under Alberta's *Societies Act* and is a "non-profit organization" as defined in section 56(1)(b)(i) of PIPA. Under sections 56(2) and (3), PIPA only applies to personal information that is collected, used or disclosed by non-profit organizations in connection with a commercial activity. Pursuant to section 56(1)(a) of PIPA, a "commercial activity" is any transaction, act, conduct, or regular course of conduct that is of a commercial character. To the extent the personal information at issue in this case was collected in connection with a commercial activity, PIPA applies.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • first and last name, • home address, • cell phone number, • email address (including business email address), • passwords.

	Corporate credit cards with employee names on the cards may have also been viewed. Information about identifiable individuals is "personal information" as defined in section 1(1)(k) of PIPA to which the Act applies. Some of the information also appears to be "business contact information" which is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business e-mail address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the loss and possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." Therefore, PIPA applies.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On November 22, 2017, the Organization's Calgary office was broken into and a number of items were stolen, including 17 laptop computers and a notebook containing some work-related information. • Three of the laptops were not encrypted, but only one had personal information stored on it (first name and last name, zone the individual worked in, and business email address). • A paper document was posted by a desk and listed personal contact information for a number of physician members. • Corporate credit cards were stored in desks but not taken.
Affected individuals	The incident affected approximately 14,043 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Reported to law enforcement and conducted an internal investigation. • Revised practices to ensure personal information is stored in locked desk drawers. • All laptops are now encrypted. • Cancelled credit cards that were potentially exposed. • Changed passwords.

	• Reviewed and enhanced physical security. • Sent staff privacy and security reminders.
Steps taken to notify individuals of the incident	On December 6, 2017, the Organization notified all physician members, contractors and employees by email. Additional notices were sent to 16 individuals on December 6, 2017 and December 15, 2017.
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 zone members contact list consisting of their names and business or personal email addresses would result in minimal harm to these individuals" and "…personal email addresses could possibly be of use to individuals interested in carrrying [sic] out a social engineering scam...". In my view, a reasonable person would consider the personal information at issue could most likely be used to cause the significant harm of phishing, which can increase vulnerability to identity theft and fraud, particularly in conjunction with other personal information elements.
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 "Keepiong [sic] in mind that the PI on the laptop's desktop consisted of first and last names and business or personal email addresses, there is no foreseen real risk of significant harm that could come to these individuals as a result of such information being exposed. While there always exists the potential for social engineering to take place with some effort made on the part of the individuals to carry out such a scam, the [Organization] has always been transparent with its members and will inform them of this breach and also provide the OIPC will the results of our findings since we contacted the OIPC upon learning of the break-in as a means to take proactive measures." With respect to social engineering, the Organization also said "…the likelihood in this case is low as it appears that the individual(s) who stole the laptops, gift card and notebook were focused on 'quick wins.' That is, stealing what they could easily access and later selling it without taking too much effort." In my view, 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 (break-in and theft). The information has not been recovered. The Organization can only speculate that the thieves were after "quick wins" and will not use the personal information at issue to cause harm.

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 in this case. A reasonable person would consider the personal information at issue could most likely be used to cause the significant harm of phishing, which can increase vulnerability to identity theft and fraud, particularly in conjunction with other personal information elements. 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 (break-in and theft). The information has not been recovered. The Organization can only speculate that the thieves were after "quick wins" and will not use the personal information at issue to cause harm. 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 the Organization notified affected individuals on December 6, 2017, by email. Additional notices were sent to some individuals on December 6, 2017 and December 15, 2017. Therefore the Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner