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	Calgary Science Centre Society (Organization)
Decision number (file number)	P2019-ND-126 (File #011233)
Date notice received by OIPC	December 19, 2018
Date Organization last provided information	December 19, 2018
Date of decision	August 7, 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 is incorporated under Alberta's *Societies Act*, and 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's website says that it provides "…interactive galleries, an outdoor park, school programs, camps, [and] professional development programs" among other things. It is not clear to me if these are commercial activities; however, to the extent the personal information at issue in this case was collected, used or disclosed in connection with any commercial activities, PIPA applies.

Section 1(1)(k) of PIPA "personal information"	The information at issue includes: • user name and address, • email address, • telephone number, • the email subject-matter, • one credit card number (no CVV, expiry date in the past), and • 4 emails related to camp attendees (including child's name, date of birth and health card number). 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 November 6, 2018, an employee of the Organization logged in to their email account from a remote location using an apparently insecure public WIFI hotspot. The employee's log-in information (username and password) were intercepted by an unauthorized third party. • The user's log-in credentials were subsequently used on more than one occasion by the unauthorized third party to gain access to and manipulate the user's email address and file folder systems, including requesting a change in bank account information for electronic payroll deposits. • The breach was detected on November 15, 2018 when the user returned to the office from vacation and confirmed that the user's email folders and emails had been tampered with. • The user's email folders were potentially exposed from November 7-15 and contained saved email correspondence. • No other system access was attempted or accomplished.
Affected individuals	The incident affected 102 individuals.
Steps taken to reduce risk of harm to individuals	• The employee's user authentication credentials were changed, email accounts were backed up and saved, the account was surveilled and available event logs were reviewed. A detailed report was subsequently prepared. • The email account was secured from further tampering.

Steps taken to notify individuals of the incident	The Organization's report of the incident said "We plan to notify each person individually by email out of courtesy to advise of the situation and the limited exposure created and to apologize; we also plan to contact the three individuals where health card information was exposed in person, by telephone."
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: *Based on the information available to date it is the [Organization's] assessment that: there is little or no potential for harm to any public institution, body or organization; there is no involvement of card or payment systems; nor any realistic potential to cause a loss of trust of any particular organization in a larger societal sense; nor any real potential risk of physical harm, security, reputational or relationship harm to the Science Centre's customers, none of whose workable payment and purchasing information was even potentially exposed.* In my view, a reasonable person would consider that the financial and identity information at issue for a limited number of affected individuals could be used to cause the significant harms of identity theft and fraud. Email addresses could also be used to cause the significant harm of phishing.
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: *The unauthorized actors have not yet been identified. There is no reason to suspect that those actors were specifically targeting the [Organization] or its customers, and every reason to suspect that this was a 'crime of opportunity' (public WIFI sniffing), although there is no denying that the malicious actor attempted to perpetrate the payroll fraud.* In my view, a reasonable person would consider that the likelihood of harm is increased as the breach resulted from deliberate, malicious action, including attempted payroll fraud, and considering the unauthorized actor had repeated access to the user's email account over the course of a week.
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 financial and identity information at issue for a limited number of affected individuals could be used to cause the significant harms of identity theft and fraud. Email addresses could also be used to cause the significant harm of phishing. The likelihood of harm is increased as the breach resulted from deliberate, malicious action, including attempted payroll fraud, and considering the unauthorized actor had repeated access to the user's email account over the course of a week.

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) and confirm to my Office, in writing, within 10 days of the date of this decision, that it has done so.

Jill Clayton
Information and Privacy Commissioner