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	McKenzie Lake Community Association (Organization)
Decision number (file number)	P2019-ND-078 (File #011749)
Date notice received by OIPC	January 21, 2019
Date Organization last provided information	June 4, 2019
Date of decision	June 5, 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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	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. "Non-profit organization" is defined in section 56(1) to mean an organization "that is incorporated under the *Societies Act* or the *Agricultural Societies Act* or that is registered under Part 9 of the *Companies Act*." In this case, the Organization is a registered non-profit organization under the *Societies Act*. The information at issue was collected in connection with an out of school program that the Organization operates and for which it charges a fee. In my view, the information was collected in connection with a commercial activity, and therefore PIPA applies.
Section 1(1)(k) of PIPA "personal information"	The Organization said that "The personal information was the parents email addresses and names, we don't know for sure but we think the phone numbers would have gone over as well". However, the Organization also said "We are not sure of all the information that was taken".

	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 11, 2018, an employee took information for children in the Organization's Before & After School program and transferred it from her company phone to her personal phone. • The breach was discovered on January 9, 2019, when parents complained to the Organization as to why the employee was now sending emails from her personal email.
Affected individuals	The incident affected 90 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	Storing information on hard copy now.
Steps taken to notify individuals of the incident	Affected individuals have not been notified.
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 harm that might result from this incident include "The potential of having 90 childrens [sic] information between the ages of six and twelve." In my view, a reasonable person would consider that the contact information at issue, including email address, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are significant harms. Because the Organization cannot identify whether other personal information was taken, it is not clear what other possible harms may exist.

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 likelihood of risk is "Unknown at this time". In my view, the likelihood of harm resulting from this incident is increased because the Organization does not know if the personal information was compromised due to negligence or malicious intent of the employee. The Organization reported it is not sure of all the personal information that was compromised, and did not ask the employee to delete the personal information or confirm that the information has not been used, copied, disclosed, or otherwise distributed. It appears from the Organization's report that the information was used to contact parents.

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 contact information, including email address, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are significant harms. Because the Organization cannot identify whether other personal information was taken, it is not clear what other possible harms may exist.

The likelihood of harm resulting from this incident is increased because the Organization does not know if the personal information was compromised due to negligence or malicious intent of the employee. The Organization reported it is not sure of all the personal information that was compromised, and did not ask the employee to delete the personal information or confirm that the information has not been used, copied, disclosed, or otherwise distributed. It appears from the Organization's report that the information was used to contact parents.

I require the Organization to notify the affected individuals 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