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	Medicine Hat Family Young Men's Christian Association (Organization)
Decision number (file number)	P2022-ND-027 (File #022532)
Date notice received by OIPC	May 18, 2021
Date Organization last provided information	May 18, 2021
Date of decision	May 11, 2022
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 reported that it is incorporated under Alberta's *Societies Act* and therefore is 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 operates health and fitness programs, day camps, and before/after school care programs. In my view, the Organization is engaging in commercial activities. To the extent the personal information at issue in this matter was collected, used and disclosed by the Organization in connection with these activities, PIPA applies.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • individuals' email address. 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	• An employee with the Organization sent an email to 10 of its members without blind carbon copying all recipients. • The Organization reviewed the email contents and reported that the content of the email itself did not contain any personal or confidential information. The email was a generic email asking recipients to log into their member portals to update payment information. • An email recipient notified the Organization of the error.
Affected individuals	The incident affected 10 individuals.
Steps taken to reduce risk of harm to individuals	• Provided a clear set of job expectations for employees that only authorized staff are allowed to send emails pertaining to payment information. • Provided training. • Coached the employee.
Steps taken to notify individuals of the incident	The affected individuals were notified by email on May 18, 2021.
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, *"If email information is sent to an unauthorized contact, there is a possibility the person's email may become hacked and their personal contacts may be affected by hackers and phishing emails."* In my view, a reasonable person would consider that the information at issue (email address associated with a notice to clients of the Organization) could be used to cause humiliation and embarrassment. Email addresses 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 the likelihood that harm will result is, *"Likelihood 1 of 5* *Exposure 4 of 5* *Consequence 4 of 5* *Total Risk Rating = 3 of 5 Medium Risk"*

	In my view, the likelihood of significant harm resulting from this incident is decreased because the incident did not result from malicious intent, but rather human error. The unintended recipients are known to the Organization and one of the recipients reported the breach. Despite this, it is not clear from the Organization's report that the Organization requested the recipients delete the email or whether the recipients confirmed deleting the email or confirmed not forwarding or otherwise using or distributing it. Further, it is not clear whether there are likely to be personal/professional relationships between the recipients such that humiliation and embarrassment might result.

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 information at issue (email address associated with a notice to clients of the Organization) could be used to cause humiliation and embarrassment. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of significant harm resulting from this incident is decreased because the incident did not result from malicious intent, but rather human error. The unintended recipients are known to the Organization and one of the recipients reported the breach. Despite this, it is not clear from the Organization's report that the Organization requested the recipients delete the email or whether the recipients confirmed deleting the email or confirmed not forwarding or otherwise using or distributing it. Further, it is not clear whether there are likely to be personal/professional relationships between the recipients such that humiliation and embarrassment might result.

I require the Organization to notify the affected individuals, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individuals by email on May 18, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Information and Privacy Commissioner