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)	P2020-ND-094 (File #016762)
Date notice received by OIPC	August 12, 2020
Date Organization last provided information	August 12, 2020
Date of decision	September 2, 2020
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. It therefore qualifies as a "non-profit organization" as defined in section 56(1)(b)(i) of PIPA. Pursuant to sections 56(2) and (3), 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 by the non-profit organization in connection with any commercial activity…". In this case, the Organization collected the information at issue in connection with registering individuals for a summer camp for which the Organization charges a fee. This appears to qualify as a commercial activity such that PIPA applies in this case.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • full legal name, and • 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	• On June 15, 2020, an employee with the Organization sent an email contact list containing guardians' contact information via the Organization's OneDrive to an unauthorized recipient (a guardian of a child) in error. • On August 11, 2020, the error was discovered, and the employee asked the unauthorized recipient to delete the email sent on June 15, 2020.
Affected individuals	The incident affected 30 individuals.
Steps taken to reduce risk of harm to individuals	• Deleted the document from the OneDrive link so that if a non-staff member tries to access the file it will not open. • Asked the unintended recipient to delete the email. • Set-up password protection for any personal information spreadsheets on its OneDrive link.
Steps taken to notify individuals of the incident	The affected individuals were not notified of the incident.
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 the person who was sent the email contact list did not delete or properly remove the file from their computer, email information may get leaked and increase the risk of malicious software attacks through phishing emails". I agree with the Organization's assessment. A reasonable person would consider that the contact information along with the email address could be used for the purposes of phishing, increasing the affected individuals' 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 of reoccurrence - Possible but not common." In my view, a reasonable person would consider that although the unauthorized disclosure was caused by human error and the email was sent to a known recipient, the likelihood of harm resulting from this incident is increased because it appears the Organization did not obtain confirmation from the unintended recipient that the email was deleted and not copied, forwarded or otherwise distributed.

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 along with the email address could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are significant harms. Although the unauthorized disclosure was caused by human error and the email was sent to a known recipient, the likelihood of harm resulting from this incident is increased because it appears the Organization did not obtain confirmation from the unintended recipient that the email was deleted and not copied, forwarded or otherwise distributed. **I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and confirm to my Office in writing, within ten (10) days of the date of this decision, that this has been done.**

Jill Clayton
Information and Privacy Commissioner