



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	YMCA Canada - Medicine Hat (Organization)
Decision number (file number)	P2022-ND-067 (File #023030)
Date notice received by OIPC	June 1, 2021
Date Organization last provided information	June 1, 2021
Date of decision	December 23, 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 <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	<p>The Organization reported that it is incorporated under Alberta’s <i>Societies Act</i> and therefore is a “non-profit organization” as defined in section 56(1)(b)(i) of PIPA.</p> <p>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.</p> <p>In this case, the Organization operates health and fitness programs, day camps, before/after school care programs, and community program. 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.</p>
Section 1(1)(k) of PIPA “personal information”	<p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none">• individuals’ email addresses. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</p>

DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none"> On May 31, 2021, an employee sent out an email to approximately 200 individuals (guardians) without blind carbon copying all recipients. The contents of the email were generic and did not contain any confidential or personal information.
Affected individuals	The incident affected approximately 200 individuals.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> Notified affected individuals. Will use a specific software program designed to prevent email addresses from being visible to any recipients. Confirm employees have the appropriate privacy training.
Steps taken to notify individuals of the incident	The affected individuals were notified by email on June 1, 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.	<p>The Organization reported the possible harms that may occur as a result of the breach is, <i>"Possibility (sic) of email being hacked and personal contacts may be affected."</i></p> <p>In my view, a reasonable person would consider that email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. This is a significant harm.</p>
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.	<p>The Organization reported that the likelihood that harm will result is,</p> <p style="text-align: center;"><i>"Likelihood 1/5 Exposure 4/5 Consequence 3.5/5 Total risk rating = 3/5"</i></p> <p>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. 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.</p>

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.

Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. This is a significant harm. 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. 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.

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 June 1, 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