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	YWCA Calgary (Organization)
Decision number (file number)	P2019-ND-013 (File #008429)
Date notice received by OIPC	April 19, 2018
Date Organization last provided information	November 28, 2018
Date of decision	February 14, 2019
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates on a not for profit basis. 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 established by a special act of the Alberta Legislature and does not qualify as a "non-profit organization" as defined in section 56(1)(b) of PIPA, despite operating on a not for profit basis. Therefore, PIPA applies in this case.

Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • email address, • possible dates and times for intake. This information is about an identifiable individual 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 March 25, 2018, a practicum student accidently forwarded an email to a client instead of a co-worker. • The client and the co-worker had the same name. • The student noticed the error the same day and tried to recall the email. • The unintended recipient was asked to delete the email; however, the Organization did not receive confirmation that this was done.
Affected individuals	The incident affected 1 individual.
Steps taken to reduce risk of harm to individuals	• Contacted the Organization's privacy counsel. • Contacted the individual who received the email in error and asked them to delete the email. • Sent an internal email to all users on how to remove the autocomplete contacts in the email.
Steps taken to notify individuals of the incident	The affected individual was notified by letter sent on March 28, 2018.
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 that the "Type of harm that could result would be identity theft". In my view, the name and email address could be used for phishing purposes. In previous breach notification decisions, I have found that phishing is a significant harm.

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 could result is very low. There was only one person who the information was sent to via the misdirected email. The information was not highly sensitive and no vulnerable individuals were involved." In my view, although the unauthorized disclosure was caused by human error and the email was accidently sent to a known unintended recipient, the likelihood of harm resulting from this incident is increased because the Organization did not receive 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 individual.

The name and email address could be used for phishing purposes. In previous breach notification decisions, I have found that phishing is a significant harm. Although the unauthorized disclosure was caused by human error and the email was accidently sent to a known unintended recipient, the likelihood of harm resulting from this incident is increased because the Organization did not receive 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 individual in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individual in a letter dated on March 28, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner