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)	P2018-ND-009 (File #006769)
Date notice received by OIPC	October 5, 2017
Date Organization last provided information	October 5, 2017
Date of decision	January 5, 2018
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"	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 the following information: • Donor information (name, address, email address, amount of donation).

	• Childcare registration packages, including:
	  ○ name and address of children and parents,
	  ○ emergency contact information,
	  ○ parents' credit card information,
	  ○ children's Personal Health Numbers,
	  ○ children's dates of birth,
	  ○ parental notes on children's general health and behaviour.
	
	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.

DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On September 14, 2017, papers containing the personal information at issue were inadvertently put in one of the Organization's general recycling bins, rather than the secured recycling bin. This is contrary to the Organization's standard secure disposal procedure. • Late in the evening of the same day, housekeeping staff disposed of the papers from the general recycling bin in an exterior, unsecured recycling dumpster. • Early in the morning of September 15, 2017, an employee arriving at work noticed papers containing personal information behind the exterior recycling bin and contacted the Organization's privacy team. • The Organization secured the information and investigated the incident. • The Organization speculates that the papers likely fell out of the recycling bin while unknown individuals searched for payable recyclables (bottles and cans).
Affected individuals	The Organization was able to identify personal information about the following individuals by reviewing information recovered from the dumpster: • 5 children residing in Alberta, their parents and emergency contacts. • 21 donors residing in Alberta. The Organization stated that there is no way of knowing whether it secured all of the documents that were improperly disposed of as there is no record of what was thrown out and what, if anything, may have gone missing prior to the documentation being secured.

Steps taken to reduce risk of harm to individuals	• Personal information was recovered as much as possible. • Reviewed the incident with relevant team members to ensure they understand appropriate disposal practices and provided additional training.
Steps taken to notify individuals of the incident	• Notification sent by mail on September 25, 2017 to parents whose credit card information was included in the childcare registration forms. • Notification sent by mail to the 21 donors on September 25, 2017. • Telephone calls to parents of the affected children and some of the donors.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to those 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 possible harms that could result from this incident include "Potential financial loss, fraud, identity theft, negative effects on a credit record." In my view, the identity (PHNs, dates of birth) and financial (credit card) information at issue could be used to cause the harms of identity theft and fraud. Information about childrens' health and behaviour could be used to cause the harms of hurt, humiliation and embarrassment. Email addresses (of donors), along with profile information (donation amounts) could be used for phishing purposes. These are all significant harms. It is unlikely emergency contact information could be used to cause 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.	In assessing the likelihood of harm resulting from this incident, the Organization reported: • "It is estimated the documents were unsecured for less than 12 hours." • "There were 26 individuals affected by the breach with five of those being young children (under age of 5)." • "It is unknown if additional documents went missing prior to being secured. The likelihood that harm could result may be significant. These documents were on the ground in a parking lot which is accessible to the public." • "Unfortunately, the organizational security camera recordings were not accessible and we are unable to confirm timing or if others interacted with the documents." • "The nature of some of the information discovered on the documents: name, contact information, address, email, Alberta Health Care number and credit card information could be the foundation of identify [sic] theft/fraud."

	• "There was no malicious intent as the documents were accidentially [sic] placed in the incorrect (unsecure) recycling bin." In my view, despite the fact the incident resulted from human error and not malicious intent, and some information was recovered, the likelihood of harm resulting from this incident is increased because the information was unaccounted for overnight and there is evidence to indicate that unknown individuals came into contact with the papers. These individuals could have viewed or copied the personal information and used it for a fraudulent or unscrupulous purpose. Further, some of the affected individuals are children, who are members of a vulnerable population. The Organization reported that there is no way of knowing whether it secured all of the documents that were improperly disposed of as there is no record of what was thrown out and what, if anything, may have gone missing prior to the documentation being secured. While it is not known what other personal information (if any) may have been exposed, it is likely to have included childcare registration packages. Therefore, there is also a risk that this information could have been viewed or copied and used for a fraudulent or unscrupulous purpose. Further, if this information existed, it has not been recovered.

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 parents, their children, and the donors in this case.

The identity (PHNs, dates of birth) and financial (credit card) information at issue could be used to cause the harms of identity theft and fraud. Information about childrens' health and behaviour could be used to cause the harms of hurt, humiliation and embarrassment. Email addresses (of donors), along with profile information (donation amounts) could be used for phishing purposes. These are all significant harms. It is unlikely emergency contact information could be used to cause significant harm.

Despite the fact the incident resulted from human error and not malicious intent, and some information was recovered, the likelihood of harm resulting from this incident is increased because the information was unaccounted for overnight and there is evidence to indicate that unknown individuals came into contact with the papers. These individuals could have viewed or copied the personal information and used it for a fraudulent or unscrupulous purpose. Further, some of the affected individuals are children, who are members of a vulnerable population.

The Organization reported that there is no way of knowing whether it secured all of the documents that were improperly disposed of as there is no record of what was thrown out and what, if anything, may have gone missing prior to the documentation being secured. While it is not known what other personal information (if any) may have been exposed, it is likely to have included childcare registration packages. Therefore, there is also a risk that this information could have been viewed or copied and used for a fraudulent or unscrupulous purpose. Further, if this information existed, it has not been recovered.

I require the Organization to notify the parents and donors in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the parents in letters dated September 25, 2017. The letters to the parents only stated that the registration packages included their credit card information. Section 19.1(1)(b)(iii) of PIPA requires that notifications to individuals include a description of the personal information involved in the loss or unauthorized access or disclosure. However, the Organization reported that follow-up phone calls with the parents did fully describe the involved personal information. Therefore, I do not require the Organization to re-notify the parents.

I understand the Organization notified the donors by mail sent September 25, 2017. The Organization is not required to notify donors again.

Because of the reasonable likelihood that similar childcare registration information may have been exposed in this incident, beyond what the Organization was able to recover, and the fact that the Organization cannot confirm what information was improperly disposed of, I require the Organization to complete an assessment in order to identify any other individuals whose personal information is likely to have been exposed as a result of this incident, to notify those other individuals in accordance with the Regulation within 10 days of the date of this breach decision, and to confirm to my Office that this has been done.

Jill Clayton
Information and Privacy Commissioner