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	Save the Children Federation, Inc. (Organization)
Decision number (file number)	P2020-ND-191 (File #017144)
Date notice received by OIPC	August 28, 2020
Date Organization last provided information	November 11, 2020
Date of decision	December 16, 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 those individuals whose personal information was collected in Alberta, pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • email address, • mailing address, • date of birth, • event participation, and • donation history, which may include scanned cheques. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On July 16, 2020, the Organization received notice that its third-party service provider, Blackbaud, had been the target of a ransomware attack.

	• The Organization reported: *We understand from Blackbaud that the incident began in February, when the hacker gained access to Blackbaud's system, and continued until May 2020, when Blackbaud discovered the hacker was attempting to carry out a ransomware attack. ... Unfortunately, the hacker was able to make a copy of some data on the system, and Blackbaud subsequently paid a ransom to the hacker to have them delete the data. ...* • The Organization also reported that it had recently migrated off Blackbaud's hosting solution; however, Blackbaud's system still housed a backup of the Organization's US supporter database, which Blackbaud reported was involved in the incident.
Affected individuals	The incident affected 25,269 Canadians, including 2,931 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	The Organization reported its service provider: • Worked with security teams, an external forensics firm and federal law enforcement to expel the attacker from its system. • Paid the ransom demand in return for assurances that all copies of data would be destroyed. • Has implemented dark web monitoring intended to detect trafficking of any of the copied data. The Organization: • Removed its data from Blackbaud's servers. • Will continue to take steps to protect supporter's data, both internally and with its third party vendors.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on September 8, 2020.
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	The Organization reported: *We have no reason to believe that any individual has suffered any significant harm as a result of this incident and believe that the risk of any such harm is low.*

with non-trivial consequences or effects.	*Given the nature of the data involved, the only conceptual risk is that someone holding the data may use it to send emails to data subjects purporting to be from [the Organizaiton].* In my view, a reasonable person would consider that the contact, identity, and profile (donation history, potentially scanned cheques) information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing, 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: *We believe that risk is unrealistic for a number of reasons. Based on descriptions of the incident from Blackbaud, the hackers' immediate objective appears to have been to conduct a standard ransomware attack in which the hackers attempted to disrupt Blackbaud's business by locking it out of its own data and servers, thereby putting the hackers in a position to demand a ransom. Although the hackers apparently did obtain a copy of some backup data as part of the ransomware attack, there is no evidence that the hackers intended to monetize any data by misusing it or by selling it. To the contrary, [the Organization] understands that Blackbaud paid the hacker to delete the data off its systems, and, according to Blackbaud, it received a confirmation that the hacker had done so.* *To date, there is no evidence that any of the information in the database has been publicly exposed by the hacker or transferred to any other parties, and both Blackbaud and [the Organization] have put in place "dark web monitoring" to detect any trafficking in the data. And, in the almost four months since this incident was announced, [the Organization] has not received any reports from data subjects of receiving any suspicious communications.* In my view, a reasonable person would consider the likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to malicious intent (deliberate, unauthorized action, ransom demand). The Organization can only speculate as to the intentions and further actions of the hackers. Although Blackbaud reported it has no reason to believe that any data was or will be misused, the Organization cannot rule out this possibility. The lack of reported incidents to date does not mitigate against future use of the information at issue to cause harm.

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, identity, and profile (donation history, potentially scanned cheques) information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to malicious intent (deliberate, unauthorized action, ransom demand). The Organization can only speculate as to the intentions and further actions of the hackers. Although Blackbaud reported it has no reason to believe that any data was or will be misused, the Organization cannot rule out this possibility. The lack of reported incidents to date does not mitigate against future use of the information at issue to cause harm. I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals in an email dated September 8, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner