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	Canadian Bible Society (Organization)
Decision number (file number)	P2020-ND-195 (File #16783)
Date notice received by OIPC	August 17, 2020
Date Organization last provided information	November 02, 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 a national religious charitable organization and 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, • address, • email address, and • donation history. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the 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 from Blackbaud, a third-party service provider, that Blackbaud had experienced a ransomware attack.

	• The Organization reported that, according to Blackbaud, the attack was discovered on May 14, 2020. The incident affected Blackbaud's back-ups, and not live operational data. Donor information resident on the back-ups from the period of February 7, 2020 to May 20, 2020 were impacted. Blackbaud paid a ransom in return for the assurance the information would be destroyed and had not been disclosed or misused.
Affected individuals	The incident affected 17,575 individuals, including 2,899 residents of Alberta
Steps taken to reduce risk of harm to individuals	• Hired a third-party team of experts to monitor the dark web. • Enhanced its security posture.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on August 14, 2020. A statement about the breach was also posted on the Organization's website on August 14, 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 with non-trivial consequences or effects.	The Organization reported "As the information affected is mainly contact and donor information, the greatest risk would be from someone impersonating CBS to solicit funds or to conduct phishing attacks". The Organization also said: *Not all personal information is of equal sensitivity and of equal risk of being the cause of significant harms.* *[The Organization] assesses the risk to individuals and donors who only have name and mailing addresses at issue to be extremely low.* I agree with the Organization's assessment. A reasonable person would consider email address, particularly in combination with contact and profile (donation history) information, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. Name and mailing address alone are unlikely to 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.	The Organization reported: *Blackbaud informed [the Organization] that they have a high level of confidence that the data ... has not and will not be misused. Dark web monitoring has seen no signs that attackers did not follow through on the destruction of information.[The Organization] assesses the risk of misuse as low but cannot be entirely excluded on the facts of*

	Blackbaud's investigation. The sensitivity of information is generally on the low end of the spectrum. *.... A low level of risk is potentially present when email information is impacted and for that reason, [the Organization] is making notification to all those impacted individuals out of an abundance of caution.* In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion, ransom demand). The Organization cannot be certain the information will not be used to cause harm, despite the fact Blackbaud paid the ransom demand.

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 email address, particularly in combination with contact and profile (donation history) information, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. Name and mailing address alone are unlikely to be used to cause significant harm.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion, ransom demand). The Organization cannot be certain the information will not be used to cause harm, despite the fact Blackbaud paid the ransom demand.

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 by email on August 14, 2020 and a notification statement was also posted on the Organization's website the same day, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner