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	Evangelical Fellowship of Canada (Organization)
Decision number (file number)	P2020-ND-115 (File #016754)
Date notice received by OIPC	August 13, 2020
Date Organization last provided information	August 13, 2020
Date of decision	October 2, 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 federally incorporated under the *Canada Corporations Act* and 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: • individual name, • email address, • mailing address, • telephone number, • donation history, and • notes about communications and meetings with donors. 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	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: *According to Blackbaud, the attack was discovered on the same day the incident occurred, May 14, 2020. The Cyber Security team, together with independent forensic experts and law enforcement, successfully prevented the bad-actor from blocking Blackbaud's system access and fully encrypting the files.* *According to Blackbaud, ransom was paid in return for the assurance the information would be destroyed and had not been disclosed or misused. The incident affected Blackbaud's back-ups, not any live operational data. Any donor information resident on the back-ups from the period of February 7, 2020 to May 20, 2020 would be impacted.*
Affected individuals	The incident affected 77,326 individuals, including 10,860 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	The Organization reported its service provider: • Prevented the bad-actor from blocking system access and fully encrypting the files. • Paid the ransom demand in return for assurances that all copies of data would be destroyed and were not further disclosed nor misused. • Hired experts to monitor the dark web for any possible suspicious activity. The Organization: • Notified affected individuals. • Is reviewing the steps taken by Blackbaud to enhance security and is currently satisfied these are appropriate.
Steps taken to notify individuals of the incident	Affected individuals who are active donors were notified by email and newsletter on July 28, 2020. A public statement was posted on the Organization's website on July 28, 2020. All affected individuals were notified by letter on August 13, 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 information, the greatest risk would be from someone using the information to impersonate someone … to solicit funds/commit fraud or to conduct phishing attacks". I agree with the Organization's assessment. A reasonable person would consider that the email address, contact and profile information (donation history, etc.) at issue could be used for the purposes of 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: *During the… investigation of the incident, Blackbaud stated that they have a high level of confidence that the data related to [the Organization] has not and will not be misused. [The Organization] assesses the risk of misuse as low but cannot be entirely excluded on the facts of Blackbaud's investigation.* 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). Although Blackbaud reported it has no reason to believe that any data was or will be misused, the Organization cannot rule out this possibility.

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 email address, contact and profile information (donation history, etc.) at issue could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms. **T**he 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). Although Blackbaud reported it has no reason to believe that any data was or will be misused, the Organization cannot rule out this possibility.

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 for whom it had email addresses in an email on July 28, 2020. All affected individuals were notified by letter on August 13, 2020. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner