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	Convoy of Hope (Organization)
Decision number (file number)	P2021-ND-314 (File #021995)
Date notice received by OIPC	June 28, 2021
Date Organization last provided information	June 28, 2021
Date of decision	March 4, 2022
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 American non-profit humanitarian and disaster relief organization that provides food, supplies, and humanitarian services to impoverished or otherwise needy populations throughout the world. 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: • full name, • address, • email address, • telephone number, • date of birth, • gender, • marital status, • employment position, • donation amount, and • redacted credit card number and credit card expiration date ranging from 2005 to 2012.

	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	• In May 2020, the Organization's cloud-based software and data hosting solutions provider, Blackbaud, discovered that it was the target of a ransomware attack. Threat actors managed to remove a subset of data from Blackbaud's self-hosted environment, which included data being processed by Blackbaud for the Organization. • On or around July 16, 2020, the Organization received a notification from Blackbaud informing it of the incident affecting the data of some of the Organization's members. • On October 9, 2020, after extensive communications, Blackbaud provided additional information to the Organization related to the potentially impacted information. • However, because the Organization was no longer a client, Blackbaud provided the information in a format that was not readable to the Organization. • The Organization worked with third-party computer specialists to obtain the information in a readable format and proceeded with a review of the information to confirm which data was potentially impacted by the Blackbaud event.
Affected individuals	The incident affected 530 individuals including 27 whose information was collected in Alberta. .
Steps taken to reduce risk of harm to individuals	• Worked with Blackbaud to determine the potential impact on the Organization's data. • Notified affected individuals and provided them with guidance on how to better protect against identity theft and fraud. • Reviewing existing policies and procedures regarding third-party vendors. • Working with Blackbaud to ensure data was appropriately removed from the system.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on June 25, 2021.

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, "The possible consequences might include the loss of confidentiality of personal data and phishing." In my view, a reasonable person would consider that, particularly in combination, the contact, identity, employment and donor information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are all 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 that it "… has no indication that any personal information has been subject to actual or attempted misuse in relation to this Incident." 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 intrusion and ransom demand). The perpetrators both accessed and stole the personal information. The Organization cannot be confident the information will not be misused, further disseminated or otherwise made available publicly.

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, particularly in combination, the contact, identity, employment and donor information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are all 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 intrusion and ransom demand). The perpetrators both accessed and stole the personal information. The Organization cannot be confident the information will not be misused, further disseminated or otherwise made available publicly.

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 the affected individuals by letter on June 25, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner