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	Opportunity International Canada (Organization)
Decision number (file number)	P2021-ND-107 (File #016695)
Date notice received by OIPC	August 11, 2020
Date Organization last provided information	August 11, 2020
Date of decision	April 7, 2021
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"	"Non-profit organization" is defined in section 56(1) of PIPA 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*." 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. In this case, the Organization is a registered non-profit organization under the *Canada Not-for-profit Corporations Act* 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 all or some of the following information: • name, • address, • email address, • telephone number (where provided), • donation history, and

	• communication preferences. 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, was the victim of a ransomware attack. • Blackbaud informed the Organization that it discovered the attack on the same day it occurred on May 14, 2020, and that it prevented the bad actor from blocking system access and fully encrypting files. • According to Blackbaud, a 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, and not any live operational data. • Any donor information resident on the back-ups from the period of February 7, 2020 to May 20, 2020 was impacted. • Blackbaud informed the Organization that there has been no indication of any impacted data being traded on the dark web.
Affected individuals	The incident affected 8,306 individuals of which 2,634 are residents of Alberta.
Steps taken to reduce risk of harm to individuals	<u>Blackbaud</u> • Assisted law enforcement and forensic experts to prevent 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 or misused. • Hired experts to monitor the dark web for suspicious activity. • Reset passwords to the database. <u>Organization</u> • Reviewed steps taken by Blackbaud to enhance its security posture and is satisfied these are appropriate.

Steps taken to notify individuals of the incident	Active donors were notified by email on August 11, 2020. The Organization reported, "Please note that active donors were notified August 11, 2020. There are approximately 1,000 individuals, including some AB residents, who have unsubscribed from receiving marketing communications; [the Organization] will thus be using a different email mechanism to contact those individuals by August 13, 2020. The content of the notice will be the same."
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 from [the Organization] to solicit funds/commit fraud or to conduct phishing attacks." In my view, a reasonable person would consider that, particularly when combined with demographic and historical donor information, the contact information at issue (names, mobile telephone numbers and email addresses) could be used for the purposes of phishing or smishing, 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 "Blackbaud informed the organization that they have a high level of confidence that the data related to the organization has not and will not be misued (sic). 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 a deliberate unauthorized intrusion by a cybercriminal. The Organization reported that the cybercriminal had already both accessed and stolen the personal information of donors. Further, the Organization can only assume that cybercriminal did not or will not misuse, disseminate or otherwise make available publicly the personal information at issue. Finally, the personal information was in the cybercriminal's possession for approximately three months.
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 when combined with demographic and historical donor information, the contact information at issue (names, mobile telephone numbers and email addresses) could be used for the purposes of phishing or smishing, 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 a deliberate unauthorized intrusion by a cybercriminal. The Organization reported that the cybercriminal had already both accessed and stolen the personal information of donors. Further, the Organization can only assume that cybercriminal did not or will not misuse, disseminate or otherwise make available publicly the personal information at issue. Finally, the personal information was in the cybercriminal's possession for approximately three months.

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 reported "there are approximately 1,000 individuals, including some AB residents, who have unsubscribed from receiving marketing communications. The Organization reported it will thus be using a different email mechanism to contact those individuals by August 13, 2020."

The Organization is not required to notify the affected individuals again if they have already been notified in accordance with the Regulation. However, I require the Organization to confirm to my office, within 10 days of the date of this decision, that all affected individuals were notified in accordance with the Regulation.

Jill Clayton
Information and Privacy Commissioner