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 Crossroads International (Organization)
Decision number (file number)	P2021-ND-111 (File #016662)
Date notice received by OIPC	August 10, 2020
Date Organization last provided information	August 10, 2020
Date of decision	March 31, 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"	The Organization is a Canadian international development organization based in Toronto and Montréal 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, • date of birth (if provided), • contact information (including postal code and telephone number), • email address, • donation history (including amount and dates), • volunteer participation, if applicable, and • event participation, if applicable. 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 was informed by its donor and financial management solutions provider, Blackbaud, of a security incident that may have involved the Organization's data. • Blackbaud reported that in May of 2020, it discovered and stopped a ransomware attack and that the attack occurred at some point between February 7 and May 20, 2020. • After discovering the attack, Blackbaud prevented the cybercriminal from blocking system access and fully encrypting files, and ultimately expelled them from the system; however, the cybercriminal removed a copy of a subset of data from the self-hosted environment. • This subset included files belonging to the Organization, with personal information of Canadian donors. • Blackbaud paid the cybercriminal's demand with confirmation that the data was destroyed. • Blackbaud asserted that they do not have any reason to believe that any data went beyond the cybercriminal or was or will be misused.
Affected individuals	The incident affected 3,176 residents of Alberta.
Steps taken to reduce risk of harm to individuals	Blackbaud: • Hired a third party to monitor the dark web as an added control to ensure that there is no future misuse of the exposed data. • Involved internal and external supports, including law enforcement, in the investigation. • Published details of the incident online on its website. Organization: • Monitoring and responding to inquiries received from affected individuals via telephone and email. • Informed affected individuals to be alert for unsolicited emails, texts or phone calls requesting personal information. • Implemented changes to prevent incident from occurring again.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on August 7, 2020. The Organization also posted a notice on its website on August 12, 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 that it "…has identified a potential risk of harm of phishing in relation to this incident." In my view, a reasonable person would consider that contact, identity and donor history information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.
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.	In its report of the breach, the Organization did not provide its assessment of the likelihood that harm may result from this incident, but its notification to affected individuals stated: *Under these circumstances, we do not believe you need to take any action, but we also ask you to be alert to "phishing" attempts by third parties where the sender refers to your relationship with us. For example, we will never ask you to send sensitive personal information to us by email.* 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 both accessed and stole the personal information at issue. The information was exposed for approximately 3 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 contact, identity and donor history information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.

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 both accessed and stole the personal information at issue. The information was exposed for approximately 3 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 notified the affected individuals by email on August 7, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner