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	Heart and Stroke Foundation of Canada (Organization)
Decision number (file number)	P2020-ND-198 (File #016570)
Date notice received by OIPC	July 31, 2020
Date Organization last provided information	July 31, 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"	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. "Non-profit organization" is defined in section 56(1) 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*." In this case, the Organization is incorporated 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: • individual name, • email address, • mailing address, • telephone number, • donation amount,

	• donation history, and • notes related to meetings with constituents/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 personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization manages personal information related to volunteer and donor relations, communications and for historical record keeping through its service provider, Blackbaud. • On July 16, 2020, Blackbaud advised the Organization that cybercriminals accessed Blackbaud's system by using the credentials of a customer who was using Blackbaud's self-hosted environment, and attempted a ransomware attack. • Blackbaud advised that it was able to successfully prevent the cybercriminal from fully blocking system access and fully encrypting files, and was able to expel the intruder from the Blackbaud system. However, the cybercriminal was able to remove a copy of a subset of data from Blackbaud's self-hosted environment, including a copy of the Organization's CRM backup. • The incident occurred between February 7 and May 20, 2020.
Affected individuals	The incident affected 7,111,322 individuals, of whom 1,057,405 are residents of Alberta.
Steps taken to reduce risk of harm to individuals	The Service Provider: • Engaged a third party to monitor the dark web to ensure there is no misuse of the accessed data. • Moving all customers to those cloud environments. • Fixed vulnerability and enhancing access management, network segmentation, deployment of additional endpoint and network-based platforms. • Adding multi-factor authentication to all self-hosted solutions. • Having all users reset their passwords regularly and will be requiring stronger passwords for a subset of its customers Organization: • Notified affected individuals and advising them to be vigilant in monitoring for email or other communication that purports to be from the Organization soliciting funds.

Steps taken to notify individuals of the incident	Affected individuals who had email addresses exposed in the breach were notified of the incident by email on July 31, 2020. A public notice was published on the Organization's website, its Twitter account and Facebook pages on July 31, 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 "The greatest risk to individuals is that email addresses might be used in a phishing attack, where a bad actor impersonates [the Organization] and attempts to solicit donations". I agree with the Organization's assessment. A reasonable person would consider that, particularly when combined with profile information (i.e. that individuals are donors to the Organization), individual names, mobile telephone numbers and email addresses could be used for the purposes of phishing or smishing, increasing the affected individuals' 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 conducted an internal investigation and involved law enforcement (FBI) as a part of the investigation. Blackbaud concluded that there is no reason to believe that the cybercriminal will misuse or disseminate the accessed data following the ransomware attack, as such actions are contrary to the "business interests" of the perpetrator. [The Organization] considers there is a risk that email addresses may be used in phishing attacks, and that such attacks could result in harm to individuals (ex: being a victim of financial fraud). The risk of misuse of an individual's name and mailing address (and likelihood of harm) is very low.* 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 and ransom demand. The Organization reported that the cybercriminal both accessed and stole the personal information of donors. The Organization can only assume that the cybercriminal did not or will not misuse, disseminate or otherwise make available publicly the personal information at issue. It appears the personal information was exposed 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 profile information (i.e. that individuals are donors to the Organization), individual names, mobile telephone numbers and email addresses could be used for the purposes of phishing or smishing, increasing the affected individuals' 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 and ransom demand. The Organization reported that the cybercriminal both accessed and stole the personal information of donors. The Organization can only assume that the cybercriminal did not or will not misuse, disseminate or otherwise make available publicly the personal information at issue. It appears the personal information was exposed 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).

Section 19.1(1) of the Regulation states that the notification must "… be given directly to the individual…" , although section 19.1(2) says "… the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

In this case, the Organization reported that it notified affected individuals who had email addresses exposed in the breach by email on July 31, 2020. The Organization also reported that a public notice was published on its website and through social media channels. Given the Organization's submissions, I accept that indirect or substitute notice as described by the Organization is reasonable in this case.

The Organization is not required to notify the affected individuals in Alberta again.

Jill Clayton
Information and Privacy Commissioner