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	St. Marys Healthcare Foundation (Organization)
Decision number (file number)	P2020-ND-194 (File #016824)
Date notice received by OIPC	August 17, 2020
Date Organization last provided information	November 10, 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"	The Organization reported it is a not-for-profit and registered charity based in St. Marys, Ontario. 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 federal *Canada Not-for-Profit Corporation 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. Nonetheless, 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: • name, • email address, • postal address, • telephone number, • gender or other demographic information (if provided), • history of relationship with the Organization (such as donation dates and amounts, and event attendance), • family member's names and contact information (if provided), • employer or business name (if provided), and • a record of communications with the Organization. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization uses a third-party service provider, Blackbaud, to manage its donor and organization data, and to communicate with various members of its community. • On July 16, 2020, the Organization received a notice from Blackbaud reporting that it had discovered and stopped a ransomware attack. However, prior to locking the cybercriminal out, the cybercriminal took a copy of the Organization's backup file, which contained certain individuals' personal information. This occurred at some point beginning on February 7, 2020 until May 20, 2020. • Blackbaud advised the Organization that it paid a financial demand in exchange for confirmation from the attackers that the extracted information was destroyed.
Affected individuals	The incident affected 22 individuals residing in Alberta
Steps taken to reduce risk of harm to individuals	The Organization reported its service provider: • Heightened its security efforts to better protect against future ransomware attacks. • Paid a financial demand in exchange for confirmation that the extracted information was destroyed. The Organization: • Notified affected individuals.

	• Notified the Privacy Commissioner of Canada. • Advised affected individuals of precautions that can be taken to reduce the risk of harm.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on August 5, 2020. The Organization also posted a notice to its website.
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 did not specifically identify the harm(s) that might result from this incident, but its notice to affected individuals said "We also encourage you to be alert for unsolicited emails, texts or phone calls requesting personal information, in particular financial information, account numbers or passwords. Always verify the identity of the requester. Most legitimate businesses will not require you to provide this information via email". In my view, a reasonable person would consider that the contact and profile information at issue (donation history, etc.), particularly in combination with email address, could be used for 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 that it "…has no reason to believe that any data went beyond the cybercriminal, will be misused, or will be disseminated or otherwise made publicly available. Blackbaud has confirmed that they have already implemented several changes to prevent this from happening again …". 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). The Organization reported that the personal information of donors and community members was both accessed and stolen and the Organization cannot confirm the information will not be misused, 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 the contact and profile information at issue (donation history, etc.), particularly in combination with email address, could be used for phishing, increasing vulnerability to identity theft and fraud. These are 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 action, ransom demand). The Organization reported that the personal information of donors and community members was both accessed and stolen and the Organization cannot confirm the information will not be misused, 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 affected individuals by email on August 5, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner