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	Hull Services (Organization)
Decision number (file number)	P2020-ND-182 (File #017156)
Date notice received by OIPC	September 2, 2020
Date Organization last provided information	September 3, 2020
Date of decision	December 8, 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 is a non-profit organization incorporated under the *Hull Child and Family Act*; as such, it 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. The Organization is, however, an "organization" as defined in section 1(1)(i) of PIPA, such that the Act applies in this matter.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • home address, • email address, • home telephone number, and • date of birth. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization reported it uses an external database called Blackbaud Raiser's Edge NXT to store information related to its donors and volunteers. • On July 16, 2020, Blackbaud informed the Organization that, in May 2020, it discovered and stopped a ransomware attack. The back up copy of the Organization's Raiser's Edge NXT and NetCommunity files were involved in the attack. • Blackbaud advised it had successfully prevented the cybercriminal from blocking its system and fully encrypting the files; however, the attackers were able to remove a copy of a subset of data from the Blackbaud environment. • Blackbaud reported it paid the ransom demand with confirmation that the data that was removed had been destroyed. • The Organization reported the breach occurred between February 7, 2020 and May 20, 2020.
Affected individuals	The incident affected approximately 7,500 individuals.
Steps taken to reduce risk of harm to individuals	The Service Provider: • Engaged a forensics team to investigate the incident. • Contacted law enforcement in multiple countries. • Hired a team to monitor the dark web to watch for any possible use of the information. The Organization: • Notified all affected individuals. • Offered credit monitoring to individuals whose records contained birth dates. • Will no longer record or keep birthdates in the database.
Steps taken to notify individuals of the incident	Affected individuals were notified by email or letter on September 8, 2020. The Organization reported that it notified those for whom it did not have current email addresses by mail on September 25, 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 harms that might result from the incident are "Identity theft, fraudulent solicitations, humiliation." In my view, a reasonable person would consider that contact and identity information could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing, increasing the 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 "The incident has a low likelihood of resulting in the financial or reputational harm to the affected individuals." 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. Blackbaud confirmed the attacker accessed and stole personal information. The Organization cannot rule out that the information will not be further used, disseminated or otherwise made available publicly. The information appears to have been exposed for over 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 contact and identity information could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing, increasing the 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. Blackbaud confirmed the attacker accessed and stole personal information. The Organization cannot rule out that the information will not be further used, disseminated or otherwise made available publicly. The information appears to have been exposed for over 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 notified the affected individuals by email or letter on September 8 and on September 25, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner