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	Blue Heron Vocational Training Centre, Athabasca (Organization)
Decision number (file number)	P2019-ND-029 (File # 004313)
Date notice received by OIPC	November 10, 2016
Date Organization last provided information	February 6, 2018
Date of decision	February 19, 2019
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 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 a registered non-profit organization under the *Societies Act*. The Organization provides support and training to individuals with a variety of disabilities, including providing manpower for other businesses. To the extent the information at issue was collected in connection with a commercial transaction, PIPA applies.

Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • date of birth, • address, • social insurance number (SIN), • AISH number, • government identity number, • financial information, • medical information (Alberta Health care number, medication, health care provider information etc.), • education and training information, • contracts, • guardian or trustee. 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	• On November 7, 2016, a staff member looking for a file on the Organization's server noticed that information had been encrypted. • The Organization found what appeared to be ransomware and further investigation revealed that the file server had been hacked and unauthorized administrative accounts had been created on the server by the hackers. • The Organization reported that the incident likely occurred after October 12, 2017.
Affected individuals	The incident may have affected 150 individuals.
Steps taken to reduce risk of harm to individuals	• Shut down computer system. • Worked with consulting company to recover data and increase security.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter dated November 9, 2016.

REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury – that could be caused to those 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 affected individuals may be at risk for "Identity theft, negative effects on credit record, damage to reputation, financial loss". I agree with the Organization's assessment. A reasonable person would consider that the contact, identity, medical, financial, and education information at issued could be used to cause the significant harms of identity theft, fraud, financial loss, and negative effects on a credit record, as well as hurt, humiliation and embarrassment.
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 "We are not sure who may have obtained information and right now we are not sure exactly how long the exposure was. The server was hacked and there was sensitive information on the server. In addition, there is information on vulnerable individuals on the server." In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because it was the result of malicious intent (deliberate action, ransomware). The length of exposure is unknown, and vulnerable individuals are affected.

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, identity, medical, financial, and education information at issued could be used to cause the significant harms of identity theft, fraud, financial loss, and negative effects on a credit record, as well as hurt, humiliation and embarrassment. The likelihood of harm resulting from this incident is increased because it was the result of malicious intent (deliberate action, ransomware). The length of exposure is unknown, and vulnerable individuals are affected.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified the affected individuals by letter dated November 9, 2016. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner