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	Ambrose University (Organization)
Decision number (file number)	P2020-ND-171 (File #016493)
Date notice received by OIPC	July 20, 2020
Date Organization last provided information	October 8, 2020
Date of decision	December 3, 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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is a private post secondary institution located in Calgary and 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: • individual name, • mailing address, • email address, • telephone number, • date of birth, • donation history, and • academic record. 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 July 16, 2020, the Organization received an email from its cloud hosting service provider, Blackbaud Inc., reporting a remote attack on Blackbaud's servers that was discovered on May 14, 2020. • Blackbaud advised the Organization that it prevented the cybercriminals from gaining full access to its systems, but the attackers did remove a copy of a subset of data, including the information at issue.
Affected individuals	The incident affected 21,691 residents of Alberta.
Steps taken to reduce risk of harm to individuals	The Organization reported that its service provider: • paid the cybercriminal's demand for ransom, with confirmation that the removed information had been destroyed, and • engaged in ongoing monitoring of dark web for data dumps in whole or part that contain the Organization's data. The Organization: • provided notice to affected individuals, • permanently removed all data from the service provider's cloud hosting environment, • subscribed to a third party service that monitors the dark web for data dumps in whole or part that contain the Organization's data and will notify users to change their secure passwords when compromised data is discovered.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on July 20, 2020. Letters were mailed to individuals who could not be contacted by email on July 21, 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 the possible harms that might result from this incident include "Identity theft, embarrassment, email phishing". I agree with the Organization's assessment. A reasonable person would consider that the contact, identity, education and donation history information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Academic information could be used to cause hurt, humiliation and embarrassment. 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 likelihood of harm resulting from this incident is "Unknown. Vendor claims that as the ransom was paid that the malicious actor deleted all copies. Vendor indicated that they have hired assistance to search dark web for data ... [The Organization] has taken the stance that there is a chance of harm and hence the report and actions detailed in the report." 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). Although the service provider reported it has no reason to believe that any data was or will be misused, the Organization cannot rule out this possibility.

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, education and donation history information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Academic information could be used to cause hurt, humiliation and embarrassment. These are all 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). Although the service provider reported it has no reason to believe that any data was or will be misused, the Organization cannot rule out this possibility.

I understand the Organization notified affected individuals in an email on July 20, 2020, and by letter on July 21, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner