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	Ridley College School (Organization)
Decision number (file number)	P2021-ND-005 (File #016906)
Date notice received by OIPC	August 19, 2020
Date Organization last provided information	October 29, 2020
Date of decision	February 16, 2021
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 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, • mailing address, • telephone number, • donation amounts and history, and • notes relating to meeting with community members/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 uses a third-party service provider, Blackbaud, who provides a CRM platform to manage information related to donors, students and alumni. • On July 16, 2020, the Organization was advised by Blackbaud that cybercriminals accessed their system by using the credentials of a customer who was using Blackbaud's self-hosted environment, and attempted a ransomware attack. The cybercriminal was able to bypass standard anti-virus controls, before detection. Blackbaud says that it successfully prevented the cybercriminal from fully blocking system access and encrypting files, and was able to expel the intruder. • The cybercriminal was able to remove a copy of a subset of data from Blackbaud's self-hosted environment, which included a copy of the Organization's records. • The incident occurred between February 7 and May 20, 2020.
Affected individuals	The incident affected 393 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	The Organization reported its service provider: • Notified law enforcement (FBI). • Engaged a third party to monitor the dark web to ensure no misuse of the accessed data. • Is adding multi-factor authentication to all of its self-hosted solutions. • Is having all users reset their passwords regularly and will be requiring stronger passwords for a subset of our customers. The Organization: • Notified affected individuals and advised them to be vigilant in monitoring for any email or other communication that purports to be from Ridley soliciting funds, as it may be fraudulent.
Steps taken to notify individuals of the incident	The Organization reported that all individuals with an email address exposed in the breach were contacted via email on July 28, 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 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 the donor information at issue in conjunction with email addresses could be used for phishing purposes,

	increasing vulnerability to the harms of 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: *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 malicious intent (deliberate, unauthorized action, ransom demand). The Organization reported that the personal information of donors was stolen and the Organization cannot confirm the information will not be misused, disseminated or otherwise made available publicly. The information appears to have been exposed over the course of 3 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 the donor information at issue, in conjunction with email addresses, could be used for phishing purposes, increasing vulnerability to the harms of 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 was stolen and the Organization cannot confirm the information will not be misused, disseminated or otherwise made available publicly. The information appears to have been exposed over the course of 3 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 the affected by email on July 28, 2020 in accordance with the Regulation. The Organization is not required to notify the individuals again.

Jill Clayton
Information and Privacy Commissioner