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	Branksome Hall (Organization)
Decision number (file number)	P2021-ND-021 (File #016545)
Date notice received by OIPC	July 27, 2020
Date Organization last provided information	July 27, 2020
Date of decision	February 23, 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 a co-educational private school offering programs in Toronto, Ontario, 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: • name, • contact information (including email address), • demographic information (including date of birth), • history of relationship with the Organization, such as past donations and amounts. 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 provider's customer relationship management (CRM) platform to support its data for alumni, parents, students and the broader community. • On July 16, 2020, the third party provider (Blackbaud) informed the Organization that its database backup had been affected by a ransomware incident, which began in February 2020, but was discovered in May 2020. • According to Blackbaud, after discovering the attack, it successfully prevented the cybercriminal from blocking system access and fully encrypting files, and ultimately expelled them from the system; however, the cybercriminal removed a copy of a subset of data from Blackbaud's self-hosted environment, including the Organization's backup. • Blackbaud paid the cybercriminal's ransom demand and received confirmation that the backup copy was destroyed. • Blackbaud indicated that based on the nature of the incident, its research, and third party (including law enforcement) investigation, it has no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly.
Affected individuals	The incident affected 74 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Working with Blackbaud to ensure the ongoing security of its database and timely updates are provided. • Currently renegotiating its contract with Blackbaud to include additional security provisions. • Requesting that Blackbaud complete a third-party privacy and security assessment. • Currently assessing all the data fields in its database to determine if certain fields should be removed or modified. • Reported this incident to Canadian privacy commissioners. • Recommend that affected individuals remain alert for communications from third parties referencing their relationship with the Organization and review bank and credit card account statements for suspicious or unauthorized activity, especially in the case of unauthorized access to the affected individual's or their child's date of birth.
Steps taken to notify individuals of the incident	Affected individuals were notified by email and letter on July 27, 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, *Considering the nature of the information compromised, [the Organization] has identified two types of risk: (i) phishing for individuals with an email address in the database and (ii) fraud for individuals with a date of birth in the database.* In my view, a reasonable person would consider that contact, identity and donor information could be used to cause the significant harms of identity theft, fraud and financial loss. Email addresses could be used for the purposes of phishing, increasing the affected individuals' 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 that it "…believes that the risk of harm is low considering that the cybercriminals objective was to receive a ransom … not to further misuse personal information removed." 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. The Organization reported that the cybercriminal both accessed and stole the personal information at issue. The Organization can only assume that cybercriminal did not or will not misuse, disseminate or otherwise make available publicly the personal information at issue. The Organization can only speculate as to the motives of the thief. Finally, the personal information may have been exposed for approximately three (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 contact, identity and donor information could be used to cause the significant harms of identity theft, fraud and financial loss. Email addresses could be used for the purposes of phishing, increasing the affected individuals' 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. The Organization reported that the cybercriminal both accessed and stole the personal information at issue. The Organization can only assume that cybercriminal did not or will not misuse, disseminate or otherwise make available publicly the personal information at issue. The Organization can only speculate as to the motives of the thief. Finally, the personal information may have been exposed for approximately three (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 notified the affected individuals by email and letter on July 27, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner