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	Ashbury College (Organization)
Decision number (file number)	P2020-ND-157 (File #016602)
Date notice received by OIPC	August 4, 2020
Date Organization last provided information	November 3, 2020
Date of decision	November 20, 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 an independent day and boarding school located in Ottawa, 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, • telephone number, • email address • mailing address, • name and contact of parent/guardian, • date of birth, • country of residence, • academic information for certain years (courses taken, grades), and • interactions with the Organization (donations, awards, events attended and committees). 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	• On July 16, 2020, the Organization was notified by its software service provider, Blackbaud, that Blackbaud had experienced a remote attack on its servers. • Blackbaud informed the Organization that it was able to expel the ransomware from its system but before it was removed, hackers were able to extract certain files that contained personal information of the Organization's constituents. • The Organization reported that it is not aware of how the ransomware entered the system or the causes of the event. • The attack occurred between February 7 and May 20, 2020.
Affected individuals	The incident affected 25,000 individuals, including approximately 197 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Advised affected individuals to remain diligent regarding their personal information. • Instructed individuals to contact the Organization or the police if they are approached by anyone regarding this incident. • Evaluating its use of third-party service providers and its internal security protocols.
Steps taken to notify individuals of the incident	Some of the affected individuals (6,800) were notified of the incident by email on July 30, 2020. For the rest of the affected individuals, the Organization proceeded with indirect notification through its website on September 1, 2020, and its Facebook page, Instagram page, Twitter account, and via its Alumni portal on September 2, 2020. On November 3, 2020, the Organization reported that on "October 29, 2020, [the Organization] provided updated email notification to the individuals whose academic information was affected in the cybersecurity incident. A total of 1,243 individuals were provided with the updated notification".

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: *Contact and identity information poses a risk of harm associated with phising (sic) attempts and fraud. Information that discloses that an individual has made donations to an institution poses a risk of harm that financial information would be made public.* I agree with the Organization's assessment. A reasonable person would consider that, particularly when combined with contact, education and profile information (e.g. that individuals are donors of the Organization), names, mobile telephone numbers and email addresses could be used for the purposes of phishing or smishing, increasing the affected individuals' vulnerability to 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, *The likelihood of harm is low given the relatively non-sensitive nature of the information…[The Organization] did not use the affected Blackbaud systems for academic information or for health information. For some students and alumni, country of birth and birth date was made available which may create a low risk of attempted fraud. For donors, the donation amounts would be considered confidential in that the information relates to personal finances/financial status.* 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 and ransomware attack. The Organization reported that the cybercriminal had already both accessed and stolen the personal information of donors. Finally, the personal information was in the cybercriminal's possession for approximately 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, particularly when combined with contact, education and profile information (e.g. that individuals are donors of the Organization), names, mobile telephone numbers and email addresses could be used for the purposes of phishing or smishing, increasing the affected individuals' vulnerability to 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 a deliberate, unauthorized intrusion by a cybercriminal and	

ransomware attack. The Organization reported that the cybercriminal had already both accessed and stolen the personal information of donors. Finally, the personal information was in the cybercriminal's possession for approximately 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).

Section 19.1(1) of the Regulation states that the notification must "… be given directly to the individual…" , although section 19.1(2) says "… the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

In this case, the Organization reported that it provided direct notification to a subset of individuals where it had current contact information. For the rest of the individuals for whom the Organization did not have updated contact information, the Organization provided substitute notice through Facebook, Instagram, Twitter, and the Organization's Alumni portal on September 2, 2020.

Given the Organization's submissions, I accept that indirect or substitute notice as described by the Organization is reasonable in this case, where the Organization is unable to contact affected individuals directly.

I understand the Organization notified the affected individuals in an email dated July 30, 2020 in accordance with the Regulation, and on its social media sites on September 2, 2020. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner