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	Saybrook University (Organization)
Decision number (file number)	P2021-ND-076 (File #017201)
Date notice received by OIPC	September 8, 2020
Date Organization last provided information	September 29, 2020
Date of decision	March 9, 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 US-based institution 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, • address, • mailing address, • telephone number, • gender, • ethnicity, • donation amounts, • marital status, • date of birth, • education history (degree, date of graduation), • donation history (gift amount, gift date, payment type, gift designation). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported, "the personal information of Albertans pertains to alumni/graduates of [the Organization] which is located in the United States, and was sent to the school in connection with

	their enrollment as students. All of these alumni were enrolled as students for in-person programs in the United States. The enrollment information could have been sent to the school through any number of means, such as through forms sent via physical mail or email to the school or online, from the United States or elsewhere. There is no definitive evidence indicating from where the enrollment information was sent." To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• In May 2020, the Organization's third party vendor, Blackbaud, advised the Organization of a data security incident involving a ransomware attack on its systems, including its Raiser's Edge software product used by the Organization. • Blackbaud reported that it was able to successfully prevent the cybercriminal from blocking its system access and fully encrypting files, and ultimately expelled them from its system. However, prior to locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from its self-hosted (private cloud) environment. • Blackbaud paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. • Blackbaud said 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 57 individuals who appear to be located in Alberta.
Steps taken to reduce risk of harm to individuals	<u>Blackbaud:</u> • published information about the incident (see https://www.blackbaud.com/securityincident). • Assured the Organization that it has taken steps to address the issue and adjusted its security measures to prevent similar issues from occurring in the future. <u>Organization:</u> • Increased its investment over the last several years to ensure ongoing alignment with industry best practices, including the use of recognized cybersecurity firms to further strengthen infrastructure.

Steps taken to notify individuals of the incident	Affected individuals were notified by email on September 8, 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 that it has "… identified a potential risk of harm of phishing in relation to this incident." In my view, a reasonable person would consider that, particularly in combination, the contact, identity, education and donor 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. 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.	In its report of the breach to my office, the Organization did not provide an assessment of the likelihood that harm may occur, but its notification to affected individuals stated: *Under these circumstances, we do not believe you need to take any action, but we also ask you to be alert to "phishing" attempts by third parties where the sender refers to your relationship with us. For example, we will never ask you to send sensitive personal information to us by email.* 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 intrusion and ransom demand). The perpetrators both accessed and stole the personal information of donors. The Organization cannot be confident the information will not be misused, further disseminated or otherwise made available publicly.
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 in combination, the contact, identity, education and donor 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. 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 intrusion and ransom demand). The perpetrators both accessed and stole the personal information of donors. The Organization cannot be confident the information will not be misused, further disseminated or otherwise made available publicly.	

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 in an email on September 8, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner