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	Norwich University (Organization)
Decision number (file number)	P2022-ND-048 (File #022061)
Date notice received by OIPC	July 2, 2021
Date Organization last provided information	July 2, 2021
Date of decision	August 29, 2022
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 based in the United States of America 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, • telephone number, • encrypted social security number, • date of birth, • donation information, • spouse name, • employment position, • profession, • marital status, • gender, and • education status. 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 is a post-secondary educational institute in Vermont, United States of Amercia. • Blackbaud Inc. (Blackbaud) provided cloud-based data management services to the Organization. • On July 16, 2020, Norwich was notified by Blackbaud that it had discovered and stopped a ransomware attack that occurred in May 2020. • Blackbaud experienced a ransomware attack that occurred between February 7, 2020 and May 20, 2020. • Blackbaud systems affected by the attack included a database containing certain data related to the Organization. • Blackbaud informed the Organization that it paid a demand to the attacker and obtained confirmation that the compromised information had been destroyed and is no longer in the possession of the attacker(s). • The Organization reported, "Due to the complex nature of the data provided by Blackbaud, this process took significant time."
Affected individuals	The incident affected 683 Canadians and 67 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	<u>Organization:</u> • Provided information to affected individuals about protecting themselves against fraud, identity theft and phishing. • Offered complimentary credit monitoring services. • Working to obtain additional information from Blackbaud regarding the steps taken to ensure that a similar incident does not occur in the future. <u>Blackbaud:</u> • Taking efforts to further secure environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter or email on June 30, 2021.

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 type of information at issue, the potential harms may include identity theft, fraud and email phishing." 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.	The Organization reported, "Norwich has no indication that any personal information has been subject to actual or attempted misuse in relation to this Incident." 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 accessed and stole the personal information of donors. The Organization cannot know if the information will 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.

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 accessed and stole the personal information of donors. The Organization cannot know if the information will 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 or letter on June 30, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Information and Privacy Commissioner