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	Brandeis University (Organization)
Decision number (file number)	P2017-ND-26 (File #001968)
Date notice received by OIPC	November 25, 2015
Date Organization last provided information	February 2, 2016
Date of decision	January 30, 2017
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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is a private research university in Massachusetts, and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • permanent address, • telephone number, • date of birth, • email address, and • student record information. Social security numbers may also have been involved. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of the information was collected from individuals residing in Alberta.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On October 26, 2015, the Organization discovered that two university computers were stolen from the Registrar's office over the preceding weekend (October 24 – 25, 2015). • The University's incident response team immediately investigated. • The information at issue was included in student account lists stored on the computers. The lists were previously deleted by the Registrar, but would have been still accessible on the device to an unauthorized user with advanced technical knowledge. • The stolen computers were password protected, but not encrypted. • The computers have not been recovered.
Affected individuals	A total of 12,373 individuals were affected, including 4 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Reviewing physical security policies. • Taking steps to ensure compliance with written Information Security Program, including encryption. • Notified law enforcement. • Notified affected individuals and provided complimentary credit reporting services.
Steps taken to notify individuals of the incident	Affected individuals were notified in writing on November 12, 2015.
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 "To date, the university is not aware of any reports of identity fraud, theft, or other harmful activity resulting from this incident, or that any personal information has actually been accessed or misused. Nevertheless, we wanted to make you (and the affected residents) aware of the incident and explain the services we are making available to safeguard the residents against identity fraud." In my view, the contact, identity and education information at issue could be used to cause the harms of identity theft and fraud, and possibly hurt, humiliation and embarrassment. Email addresses could be used for phishing purposes. 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 that "is not aware of any reports of identity fraud, theft, or other harmful activity resulting from this incident, or that any personal information has actually been accessed or misused." Further, "the computers were password-protected pursuant to university policies and the personal information could only be accessed if the password was known to the criminal. Even then, the personal information was deleted from the systems and would be difficult to recover." In my view, there is a real risk of harm resulting from this incident. The incident is the result of malicious intent (theft), the computers were not encrypted, and have not been recovered. I do not believe that the lack of reported incidents of identity theft to date is a factor in the likelihood of harm resulting from this incident, as identity theft can happen months and even years after a data breach.

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 and education information at issue could be used to cause the harms of identity theft and fraud, and possibly hurt, humiliation and embarrassment. Email addresses could be used for phishing purposes. These are significant harms. The incident is the result of malicious intent (theft), the computers were not encrypted, and have not been recovered. I do not believe that the lack of reported incidents of identity theft to date is a factor in the likelihood of harm resulting from this incident, as identity theft can happen months and even years after a data breach.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individuals in writing on November 12, 2015 in accordance with the Regulation. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner