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	University of Mary (Organization)
Decision number (file number)	P2019-ND-138 (File #012467)
Date notice received by OIPC	March 12, 2019
Date Organization last provided information	March 12, 2019
Date of decision	August 14, 2019
Summary of decision	There is a real risk of significant harm as a result of this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify the affected individual whose information was collected in Alberta.
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is a private university in Bismarck, ND, 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, and • medical information. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 30, 2019, the Organization concluded an investigation concerning suspected unauthorized access to an employee's email account. • The Organization reported the breach occurred on August 15, 2018 and ended on August 20, 2018, when steps were taken to secure the account. The Organization conducted a preliminary investigation at the time, but was unable to determine which emails or attachments may have been viewed in the account.

	• The Organization recently began a new investigation with the assistance of a forensic firm. This investigation was also unable to determine which emails and attachments may have been viewed by the unauthorized person. Therefore, the University conducted a review of the full contents of the account and determined on February 22, 2019 that an email or an attachment that could have been viewed by the unauthorized person contained the name and medical information of one Alberta resident.
Affected individuals	The incident affected 193 individuals, including one resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Providing notice and a call center to provide the affected Alberta resident with information on steps that he can take to help protect his personal information. • Over the last year, offering preventative training in cybersecurity for all employees. • Implementing additional procedures, education, and training to further enhance and strengthen its security processes.
Steps taken to notify individuals of the incident	The affected individual was notified by letter on March 12, 2019.
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 the potential harms that might result from this breach include "…emabrassment [sic] and reputational harm as a result of the potential unauthorized access to the personal information". I agree with the Organization's assessment. A reasonable person would consider that medical/health information could be used to cause the significant harms of hurt, humiliation and embarrassment.
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 resulting in this case is "Findings from the investigation indicate that the unauthorized individual utilized a phishing scheme to attempt to perpetrate wire fraud against the [Organization]. As there is no conclusive evidence that the unauthorized individual actually viewed any personal information on the Alberta resident, it is unlikely that the information would be disclosed to any additional parties that would cause the Alberta resident to experience the harms listed in the previous answer." In my view, a reasonable person would consider that the likelihood of harm resulting in this case is increased because the breach

	resulted from malicious intent (phishing scheme, attempted fraud). Although the Organization reported "there is no conclusive evidence that the unauthorized individual actually viewed any personal information on the Alberta resident", the Organization did not provide any evidence, such as audit logs, to suggest the unauthorized individual did not access the individual's information after compromising the account. Further, the Organization can only speculate as to the unauthorized individual's intent.

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 in this case.

A reasonable person would consider that medical/health information could be used to cause the significant harms of hurt, humiliation and embarrassment. The likelihood of harm resulting in this case is increased because the breach resulted from malicious intent (phishing scheme, attempted fraud). Although the Organization reported "there is no conclusive evidence that the unauthorized individual actually viewed any personal information on the Alberta resident", the Organization did not provide any evidence, such as audit logs, to suggest the unauthorized individual did not access the individual's information after compromising the account. Further, the Organization can only speculate as to the unauthorized individual's intent.

I require the Organization to notify the affected individual whose information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the affected individual was notified by letter on March 12, 2019. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner