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	College of Licensed Practical Nurses of Alberta (Organization)
Decision number (file number)	P2021-ND-278 (File #017972)
Date notice received by OIPC	November 9, 2020
Date Organization last provided information	May 26, 2021
Date of decision	February 16, 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 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, • username (LMS ID number), • encrypted password, • email address, and • course and certificate information. 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 uses a Learning Management System (LMS), hosted by a third party service provider, Steppingstones Partnership, Inc. (Steppingstones). Steppingstones leases web servers and services from another third party, Web Hosting Canada. • On October 14, 2020, Steppingstones received a notification from Web Hosting Canada concerning a security issue impacting one of their services. • Several law enforcement agencies also discovered the incident on October 14, 2020, via a tweet that identified the compromised web address, and notified the Organization. • On the same day, the Organization's third party service provider took action to quarantine several malicious files and investigate. It found that an unauthorized party uploaded several malicious executable files to the Organization's LMS on October 13, 2020. The Organization was not able to determine how the unauthorized actor breached the environment.
Affected individuals	The incident affected 9,585 individuals.
Steps taken to reduce risk of harm to individuals	• Worked with service provider to contain and analyze the breach. • Provided a sample of the malicious executables and log files to the Canadian Centre for Cyber Security. • Liaised with law enforcement agencies who reported the incident to the Organization. • Third party service provider adjusted various security settings and updated server software, hardening the web environment. • Changed administrative passwords.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on October 23, 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: *[It] is unlikely the nature of the information at issue will lead to a real risk of identity theft, embarrassment, or other significant harms. No credit information is at issue that would lead to fraudulent banking activity.* In my view, a reasonable person would consider that email addresses, in conjunction with knowledge that the affected individuals are members of the Organization, could be used for the purposes of phishing, increasing 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: *We emphasize that the categories of personal information listed above cover the information that would have been stored on the server, but the CLPNA has received no evidence to suggest that there was an unauthorized access, collection, use or disclosure of the personal information. Additionally, no personal information has been modified or lost as a result of the Breach.* *There is a very remote possibility that there was an unauthorized access, collection, use, or disclosure of personal information that was not detected … during the investigation process. However, it is unlikely the nature of the information at issue will lead to a real risk of identity theft, embarrassment, or other significant harms. No credit information is at issue that would lead to fraudulent banking activity.* *The [Organization] recognizes that the use of malware is an indicator of potential malicious intent. This led to its decision to notify all HCAs that had signed into the Bridge Modules or Working in Alberta Modules in order to increase their vigilance in detecting suspicious activity.* ***It is unclear exactly how the Malicious Files were introduced into the server.*** [emphasis added] The Organization's third party breach report states: *Was any of the data on the [LMS] site compromised? No. We have not seen any indication of [LMS] data compromised.* *Was the intruder able to view or access any of the members' data? No.* ***We believe that the intruder was able to upload the 3 malware files via FTP****. The member data is stored in a database which is not accessible via FTP. The FTP will only give the intruder access to the files (which are for the most part standard [LMS] files that can be downloaded from the [LMS] website) NOT to any data.* [emphasis added] The third party incident report also states: *I went through the RAW Log files and found every hit on the .exe files.* ***Unfortunately, this did not tell me how the files got onto your server.***

	I went through the September FTP Log files, and the only IP address using FTP in September was my own IP Addresses. ***I didn't find October FTP Log Files****.* [emphasis added] In my view, the likelihood of harm resulting from this incident may be reduced as the third party investigation found no indication that the information stored in the LMS was accessed. Despite this, I note the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion, uploading malicious files). Further, the Organization was unable to determine the root cause of the breach (log files inconclusive), could not rule out the possibility that personal information was accessed, and the extent of unauthorized access the threat actor may have had prior to containment of the breach is unclear.

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 email addresses, in conjunction with knowledge that the affected individuals are members of the Organization, could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident may be reduced as the third party investigation found no indication that the information stored in the LMS was accessed. Despite this, I note the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion, uploading malicious files). Further, the Organization was unable to determine the root cause of the breach (log files inconclusive), could not rule out the possibility that personal information was accessed, and the extent of unauthorized access the threat actor may have had prior to containment of the breach is unclear.

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 affected individuals in an email dated October 23, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner