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	Morneau Shepell Ltd. (Organization)
Decision number (file number)	P2021-ND-137 (File #015775)
Date notice received by OIPC	May 6, 2020
Date Organization last provided information	May 6, 2020
Date of decision	May 25, 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 the 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, • contact information, • date of birth, • name of clinician or practitioner, • employer information, • reported health condition, • treatment or counselling information, • age information, • race, • complaint information, • disciplinary information, • occupational information, • prescription medication information, • reason for school absence, • school information, and • username/password information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.

	The Organization reported that the types of information involved varied from user to user. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• Around January 30, 2020, the Organization discovered that multiple unauthorized emails were sent externally from the email account of an employee of the Organization. • The Organization investigated and found that the email accounts of five (5) of its employees were compromised as a result of a phishing campaign giving the unknown attacker access to email stored between January 30 and February 4, 2020. • The investigation found no evidence that personal information is being used inappropriately as a result of this incident.
Affected individuals	The incident affected 622 individuals of whom 42 were residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Investigated and retained a third party forensics firm to analyze the incident and assess the potential impact. • Engaged legal counsel specializing in cybersecurity and privacy law. • Disabled employee accounts identified as having suspicious activity and reset all employee passwords. • Undertook a comprehensive audit to determine what information was involved. • Rolled out multi-factor authentication for all employees. • Enhanced information security tools. • Adjusted phishing training exercises. • Established a call centre to address any questions. • Reported the incident to the Toronto Police Service Cyber Crime unit.
Steps taken to notify individuals of the incident	Affected individuals were notified either by email or telephone beginning the first week of May 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	The Organization reported that, "Some of the possible harms include reputational harm and embarrassment." In my view, a reasonable person would consider that the contact and identity information at issue could be used to cause the harms of identity theft and fraud. The medical and educational

important, meaningful, and with non-trivial consequences or effects.	information could be used to cause the harms of hurt, humiliation and embarrassment. 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 that the likelihood that significant harm will result is "low to moderate." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (successful phishing campaign). The Organization said it has no evidence that the information was being used inappropriately; however, the compromised information may well have continuing value over time. Further, the information may have been exposed for approximately one week.

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 the contact and identity information at issue could be used to cause the harms of identity theft and fraud. The medical and educational information could be used to cause the harms of hurt, humiliation and embarrassment. These are all significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (successful phishing campaign). The Organization said it has no evidence that the information was being used inappropriately; however, the compromised information may well have continuing value over time. Further, the information may have been exposed for approximately one week.

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 by email or telephone beginning the first week of May 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner