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)	P2018-ND-156 (File #010315)
Date notice received by OIPC	November 5, 2018
Date Organization last provided information	November 5, 2018
Date of decision	December 3, 2018
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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported that the type of personal information that may have been viewed or accessed as part of the incident varies for each individual and may include (in various combinations): • name, • date of birth, • address, • name of beneficiary, dependant and/or spouse, along with their date of birth, • name of employer, • employment information such as Employer ID, tenure and job title, • benefit plan information, including type of coverage, • pension plan information such as pension entitlements and amounts, • gender, • salary, • telephone number, and • social insurance number.

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• Between August 29 and September 5, 2018, the Organization was subject to a targeted email phishing attack that resulted in an unknown third party briefly gaining access to the email accounts of two of the Organization's employees and using those accounts to send out further phishing emails. • The Organization has determined that through a subsequent investigation that an employee clicked on a malicious link contained within a phishing email that linked to a credentials harvesting website which allowed the third party to access the employee's email account. • On our around September 5, 2018, the unknown third party sent a phishing email from the employee's email account to various internal and external recipients in the employee's email address list. A second employee within the Organization clicked on the link contained within the email allowing the third party to temporarily access the second employee's email account. • On September 6, 2018, a second phishing email was sent by the third party using the second employee's email account to all recipients in the second employee's email address book. • The incident was discovered upon the first phishing email being sent out from the first employee's email account and being forwarded to the Organization's IT security team. • On or around October 3 and 4, 2018, the Organization discovered that the incident may have resulted in access to personal information.
Affected individuals	The incident affected approximately 17,500 individuals located in Alberta and British Columbia.
Steps taken to reduce risk of harm to individuals	• Quarantined the email accounts and notified all recipients of the phishing emails to ensure they were not spread further. • Investigated internally and retained a third party forensics firm to investigate the cause and scope of the incident. • Will offer affected individuals credit monitoring at no cost to them and access to fraud prevention resources. • Set up a call centre affected individuals can contact if they have any questions.

	• Will provide employees with additional cyber security awareness training, and currently making changes to the way personal information is processed to ensure that employees avoid transferring and keeping personal information in emails. • In the process of implementing multi-factor authentication and URL reputation filtering for mail gateway. • Enhanced monitoring for suspicious activity, including email phishing attacks. Exploring options to implement a solution that will identify external sites attempting to harvest employee credentials. • Reported the breach to the British Columbia Privacy Commissioner, the Federal Privacy Commissioner, the RCMP and the Vancouver Police.
Steps taken to notify individuals of the incident	The Organization reported that "All affected individuals will be sent written notification of the Incident over the next few weeks once the Organization has confirmed the number of individuals impacted and the type of personal information associated with each individual…".
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 that "…the unauthorized access to the personal information of the employees of clients of the Organization (assuming the unauthorized access occurred) could potentially be used to conduct identity theft and/or fraud. Additionally, in the unlikely event the salary information of the individuals is publically disclosed as part of the Incident (in particular to other coworkers), it is possible that those employees may suffer from humiliation/embarrassment by having their salary information disclosed publically." I agree with the Organization's assessment. The comprehensive contact, identity and employment information could be used to cause the harms of identity theft and fraud. Employment information could be used to cause the harms of hurt, humiliation and embarrassment. The email addresses that were accessed could (and were) used for phishing purposes. 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 harm may occur to any of the affected individuals is moderate. The Incident occurred as a result of a phishing attack that involved the malicious intent on the part of an unknown third party. While the Organization currently has no evidence that the personal information of an individual has been viewed or accessed or that any individual has suffered harm as a result of the Incident, the malicious nature of the Incident would suggest that the intent was to obtain personal and financial information of individuals to use for improper purposes which increases the likelihood that harm may result at some point." In my view, the likelihood of harm resulting in this case is increased because the incident is the result of deliberate, malicious action, and appears to have targeted the information for improper purposes. The information was used to send further phishing emails.

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 comprehensive contact, identity and employment information could be used to cause the harms of identity theft and fraud. Employment information could be used to cause the harms of hurt, humiliation and embarrassment. The email addresses that were accessed could (and were) used for phishing purposes. These are all significant harms.

The likelihood of harm resulting in this case is increased because the incident is the result of deliberate, malicious action, and appears to have targeted the information for improper purposes. The information was used to send further phishing emails.

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) and **confirm to my office in writing within 10 days of the date of this decision that it has done so.**

Jill Clayton
Information and Privacy Commissioner