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	Johnston Group Inc. (Organization)
Decision number (file number)	P2021-ND-162 (File #018414)
Date notice received by OIPC	November 27, 2020
Date Organization last provided information	November 27, 2020 / June 2021
Date of decision	August 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 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. The Organization's head office is in Winnipeg, Manitoba.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • full name, • email address, • client portal name account, and • summary of benefits. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• The Organization is an employee benefits plan administrator and its client portal allows individuals to submit and track medical claims through their employers' plan.

	• On November 9, 2020, the Organization was subject to a brute-force attack against the Organization's client portal. • The actors were trying to gain access to client accounts by trying to log in with various account names (many of which were invalid). • The Organization determined that the login attempts came from a variety of computers around the world. • Five accounts were successfully compromised this way and personal information about seven individuals who reside in Alberta was accessed. • The attacker is not known.
Affected individuals	The Organization reported the incident affected seven (7) individuals who reside in Alberta.
Steps taken to reduce risk of harm to individuals	• Forced a password change on all client portal accounts that were attacked. • Advised affected individuals to change their password anywhere it has been re-used and to make sure that their passwords are unique. • Offered the services of their security team to affected individuals to help them with questions and problems that they might have. • Offered to pay for three years of credit / identity protection for each affected individual. • Changed the client portal so that similar attacks would be blocked. • Putting measures in place to detect large-scale attacks against client portal credentials that result in large numbers of locked accounts. • All client portal account owners, not just the ones involved in the recent attack, are being forced to change their passwords so that they are more complex and more resilient to future attacks.
Steps taken to notify individuals of the incident	Five (5) affected individuals were notified by telephone and a follow-up email was sent on November 13, 2020. Two (2) individuals were notified by letter sent by courier on November 19, 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: *Victims re-using their client portal passwords on other websites could experience attacks against their accounts on those sites. The harm would vary depending on the site.* *Victims whose email accounts were exposed could received targeted phishing email.* In my view, a reasonable person would consider the contact, and credentials could be used to cause the significant harms of identity theft, and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. 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: *The likelihood of harm caused by re-use of the guessed-at client portal password is moderate. Malice was involved in this attack and it is reasonable to assume that harm was the intention of the attackers. The likeliness of harm will also depend on the degree of password re-use and the security features applied to those accounts.* 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 (deliberate intrusion). The information was exposed for two (2) days.

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 the contact, and credentials could be used to cause the significant harms of identity theft, and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. 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 (deliberate intrusion). The information was exposed for two (2) days.

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 five (5) affected individuals by telephone and a follow-up email was sent on November 13, 2020. Two (2) individuals were notified by letter sent by courier on November 19, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner