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	Leede Jones Gable Inc. (Organization)
Decision number (file number)	P2021-ND-181 (File #017952)
Date notice received by OIPC	November 6, 2020
Date Organization last provided information	November 6, 2020
Date of decision	September 2, 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.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • social insurance number, • date of birth, • account number, and • account balance. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On September 27, 2020, the Organization was the victim of a ransomware attack. The incident was discovered the same day when employees were unable to remotely access some systems. • The attacker used compromised account credentials to access the Organization's network over a VPN and then deployed post-exploitation tools and ransomware. • The attacker encrypted a number of the Organization's servers, PCs, and exfiltrated data. Exfiltrated records were published on the dark web for four days prior to being taken down.
Affected individuals	The incident affected 12,090 individuals, including 2,638 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged cyber security experts to contain and investigate the incident. • Reported the incident to law enforcement and the Investment Industry Regulatory Organization of Canada. • Reset passwords across the Organization. • Reiterated that multifactor authentication is required. • Reimaged impacted systems and deployed additional software security measures. • Exploring additional security technologies. • Offered individuals two years of credit and dark web monitoring, as well as identity theft insurance.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter and telephone on October 30, 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 the breach could result in the possible harms of "Identity theft, fraud". Notifications to affected individuals also included advice on identifying and avoiding email or text phishing. I agree with the Organization's assessment. A reasonable person would consider the contact (name, address), identity (date of birth, social insurance number), and financial information at issue could be used to cause the harms of 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: *[The] risk of harm is low to medium because while the information was sensitive, it was accessible on the attacker's website for a short period of time (i.e., four days) before it was taken down.* In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unauthorized third party (deliberate intrusion and installation of ransomware). Despite the Organization reporting that exfiltrated records were taken off the dark web after four days, the personal information at issue was publicly exposed and may have been accessed by other unauthorized parties.

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 (name, address), identity (date of birth, social insurance number), and financial information at issue could be used to cause the harms of identity theft and fraud. These are 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 unauthorized third party (deliberate intrusion and installation of ransomware). Despite the Organization reporting that exfiltrated records were taken off the dark web after four days, the personal information at issue was publicly exposed and may have been accessed by other unauthorized parties.

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 by letter and telephone on October 30, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner