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-128 (File #016490)
Date notice received by OIPC	July 16, 2020
Date Organization last provided information	July 16, 2020
Date of decision	May 12, 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 Organization reported the incident involved the following information: • business contact information, and • client contact information, including SIN and date of birth in some cases related to RESP financial contributions. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. "Business contact information" is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business e mail address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose."

	In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As a result, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On or about June 2, 2020, attackers gained unauthorized access to an employee's email mailbox as a result of a phishing email that the employee responded to, providing credentials. • While accessing the account, the perpetrators emailed four other employees, making a fraudulent plea for funds. The attack was unsuccessful and immediately aroused suspicion. • The unauthorized access was terminated June 4, 2020. • The Organization's investigation confirmed access to five (5) emails within the compromised account, containing personal information of 22 individuals. • The Organization confirmed that the attacker did not forward any emails or create any forwarding rules for the employee's inbox. The investigation found no evidence of malware and that the attacker did not gain access to computer systems.
Affected individuals	The incident affected 22 individuals, including 2 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Locked the account, reset password, performed trace audits, strengthening access controls, and implementing two-factor authentication. • Retained external forensic firm to investigate. • Increased cyber security training. • Confirmed all Office 365 accounts have multifactor authentication enabled and configured. • Informed business partner institutions. • Offered credit monitoring and identity theft insurance for 12 months.
Steps taken to notify individuals of the incident	The affected individuals were notified by letter and email sent on July 16, 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 possible harms that could arise in this case are further phishing attacks, fraud and identity theft." In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing 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 fact that a threat actor gained unauthorized access via a phishing attack (originating at another financial advisory firm), in our view, indicates some risk of future phishing attacks or fraud attempts using the accessed information. That said, the bad actor did not send any phishing emails during the short period of access, opting only to attempt a fraudulent plea for funds.* 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 into an employee's email account). The Organization said, "the bad actor did not send any phishing emails during the short period of access", however, the perpetrators attempted fraud. Further, the information may have been exposed for approximately two 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 that the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing 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 into an employee's email account). The Organization said, "the bad actor did not send any phishing emails during the short period of access", however, the perpetrators attempted fraud. Further, the information may have been exposed for approximately two 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 the affected individuals by letter and email sent on July 16, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner