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	Letko, Brosseau & Associates Inc. (Organization)
Decision number (file number)	P2021-ND-312 (File #021900)
Date notice received by OIPC	June 25, 2021
Date Organization last provided information	December 10, 2021
Date of decision	March 4, 2022
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 some or all of the following information: • name, • address, • email address, • telephone number, • social insurance number, and • date of birth. 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	• On May 2, 2021, the Organization discovered it was the target of a ransomware attack by an external individual, resulting in most of its production systems being encrypted. • The Organization reported that it took all measures to block the unauthorized access, contain the incident and prevent a recurrence were implemented immediately. • The Organization's investigation revealed the REvil ransomware group perpetrated the attack and work files were exfiltrated.
Affected individuals	The incident affected 20 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Retained external cybersecurity specialists to investigate the incident. • Blocked the unauthorized access, contained the incident, and implemented processes to prevent a reoccurrence. • Offered free credit monitoring service for a 5-year period. • Notified regulatory authorities. • Implemented reinforced measures to guard against future attacks or remnants from this event.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on May 4, 2021 and November 25, 2021.
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 nature of the personal information potentially accessed, particularly the social insurance number which is sensitive, poses a risk of being used to cause harm, notably identity theft.* In my view, a reasonable person would consider the contact and identity 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 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: *To date, there has been no misuse for fraudulent purposes, such as identity theft, that [the Organization] has been made aware of. As a result, and considering the measures taken to contain the incident as well as those taken to help prevent fraud against the affected … clients, we assess the risk of harm as low for such individuals.*

	In my view, a reasonable person would consider 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, ransom demand). In this case, the information at issue was accessed and stolen. Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the compromised information were to be used for fraudulent purposes. Finally, it is unclear how long the information may have been accessible to the threat actors.

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 identity 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 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, ransom demand). In this case, the information at issue was accessed and stolen. Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the compromised information were to be used for fraudulent purposes. Finally, it is unclear how long the information may have been accessible to the threat actors.

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 on May 4, 2021 and November 25, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner