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	Lachman Consultant Services, Inc. (Organization)
Decision number (file number)	P2022-ND-065 (File #023610)
Date notice received by OIPC	October 15, 2021
Date Organization last provided information	March 4, 2022
Date of decision	November 18, 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 located in Westbury, NY, USA, and 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, • Social Security Number, • Telephone number, • email address, • payroll information, and • dependent and beneficiary names, addresses, telephone numbers, and Social Security numbers. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent that the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization was victim to a ransomware attack. • Unauthorized activity was first detected on the Organization's

	network on or about on August 10, 2021; on August 21, 2021, the Organization determined "this was a security issue." • An investigation determined that a "threat actor compromised an employee's credentials to gain network access." • A February 16, 2022 update states: "Personal information appears to have been exfiltrated."
Affected individuals	The incident affected 1,940 individuals, including 2 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged incident response firms. • "Arranged for affected individuals to receive … identity theft protection services." • Accelerated information technology upgrades to improve protection of data. • Ongoing monitoring of "activity resulting from the incident."
Steps taken to notify individuals of the incident	Affected individuals, including beneficiaries and dependents, were notified by letter on September 21, 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 on October 15, 2021: *Personal information of affected individuals could be misused.* When asked to elaborate on possible harms, the Organization reiterated on February 16, 2022: "Personal information of any individuals that may potentially be affected could be misused". In my view, a reasonable person would consider that identity (Social Security Number), contact, dependent/beneficiary, and payroll information could be used to cause the 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 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 on October 15, 2021: *As of this notice, [the Organization] is not aware of any misuse of the compromised personal information as a result of this incident. While [the Organization] believes the incident has been contained, [the Organization] is taking steps to maintain the security of any data potentially impacted and continues to monitor for any activity resulting from the incident.*

	When asked for an updated assessment on the likelihood that significant harm would result, the Organization reiterated on February 16, 2022: *Personal information of any individuals that may potentially be affected could be misused, but [the Organization] has arranged for affected individuals to receive 24 months of free identity theft protection services…* *[The Organization] is not aware of any misuse of the personal information resulting from this incident. While [the Organization] believes the incident has been contained, [the Organization] continues to take steps to maintain the security of any data potentially impacted and monitor for any harm resulting from the incident.* *Moreover, [the Organization] has engaged an outside cyber security specialist to continue to monitor for any misuse of personal information and that specialist has confirmed that there has been no occurrence of misuse observed to date.* 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 a threat actor (deliberate intrusion, deployment of ransomware, exfiltration of personal information). The lack of reported misuse of personal information does not mitigate future harm as phishing, fraud, and identity theft can occur months or years after a breach.

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.

Identity (Social Security Number), contact, dependent/beneficiary, and payroll information could be used to cause the 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 significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a threat actor (deliberate intrusion, deployment of ransomware, exfiltration of personal information). The lack of reported misuse of personal information does not mitigate future harm as phishing, fraud, and identity theft can occur months or years after a breach.

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 September 21, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance