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	Olymel LLP (Organization)
Decision number (file number)	P2021-ND-011 (File #018307)
Date notice received by OIPC	November 23, 2020
Date Organization last provided information	December 21, 2020
Date of decision	February 16, 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, • date of birth, • social insurance number, and • passport number (foreign workers). 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 September 19, 2020, a criminal organization attempted to access the Organization's systems.

	• The Organization became aware of the attack on or about October 5, 2020, when certain systems started to encrypt, affecting the Organization's operations. • On October 16, 2020, the Organization paid a ransom and in return received delete logs, which provide evidence that all exfiltrated files (including all files containing personal information) have been securely deleted.
Affected individuals	The incident affected 80,047 individuals, including 106 in Alberta.
Steps taken to reduce risk of harm to individuals	• Mobilized the Organization's crisis unit and brought together stakeholders from senior management, communications and the IT security team. • Retained lawyers and experts to guide the crisis unit and strengthen the security of IT systems. • Identified the source of the security breach and followed the recommendations of security experts to correct the breach. • Conducted darkweb searches, which did not reveal any public disclosure to date. • Offered a credit monitoring service. • Notified data protection authorities. • Implemented additional security measures.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter during the week of December 7, 2020. The Organization also notified the employees' union prior to sending the written notice to affected individuals.
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 "Possible financial harm" might result from the breach. In my view, a reasonable person would consider the contact and identity information at issue could be used to cause the significant harms of identity theft, and fraud.
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 that the harm will result is relatively low. Although the threat actors exfiltrated data … they do not appear to have been specifically targetting [sic] personal information. In fact, according to expert analysis, the vast major of the exfiltrated files (roughly 99%) did not contain personal information.*

	Instead, the threat actors appear to have sought immediate financial gain. A ransom was also paid to the criminals on October 16, 2020, and they provided delete logs, which provide evidence that all exfiltrated files (including all files containing personal information) have been securely deleted. *Darkweb searches conducted by experts also do not reveal that there has been any public disclosure to date.* The Organization also reported, "Of course, no organization that has been victim of such an incident can ever be certain whether the criminals did (or did not) view, copy to otherwise distribute such information prior to deletion". 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). The Organization can only speculate as to the motives of the perpetrators. The Organization acknowledged that it can not be certain the perpetrators did not view, copy, or otherwise distribute the information.

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 significant harms of identity theft, and fraud. 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). The Organization can only speculate as to the motives of the perpetrators. The Organization acknowledged that it cannot be certain the perpetrators die not view, copy, or otherwise distribute the information.

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 during the week of December 7, 2020. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner