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	Royal Camp Services Ltd. and its subsidiaries and affiliates Summit Camp Services Ltd. and Chief Isaac Summit Camp Services Ltd. (Organization)
Decision number (file number)	P2021-ND-198 (File #018574)
Date notice received by OIPC	December 7, 2020
Date Organization last provided information	December 7, 2020
Date of decision	October 15, 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, • email address (if provided), • telephone number, • social insurance number, • date of birth, • hire date, • termination date, and • banking information (institution and account number). 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 August 26, 2020, the Organization was the victim of a cybersecurity attack by an unauthorized third party who deployed ransomware and encrypted parts of the Organization's technology infrastructure. • The Organization discovered that the unauthorized third party may have gained access to the personal information of current and former employees of subsidiaries and affiliates. • The Organization reported there was no evidence of exfiltration of files. • The Organization determined that the unauthorized user had access to its systems between August 13-26, 2020. • The Organization reported there is no evidence of its data being available on the deep or dark web or evidence related to any attacks.
Affected individuals	The incident affected 3,986 individuals, including 1,959 individuals whose personal information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Investigated, including to determine the extent of the breach, and implemented an incident response plan, including ensuring the external actor no longer had access to systems. • Arranged for identity theft and credit monitoring services for affected individuals for a period of 24 months. • Implemented additional information security measures. • Conducted a review of security and cybersecurity measures with a third part forensic IT firm. • Reviewing cybersecurity and privacy policies and procedures.
Steps taken to notify individuals of the incident	Affected individuals were notified either by letter on December 3, 2020 or by email on December 7, 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 "...there are potential risks of identity theft, fraud and financial loss and embarrassment and phishing attack for the individual [sic] affected in Alberta". I agree with the Organization's assessment. A reasonable person would consider the contact, identity, financial and employment information at issue could be used to cause the significant harms of identity theft, fraud, financial loss and embarrassment. 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 likelihood that harm could result is low to moderate. While [the Organization] has no evidence that the personal information at issue has been misused by the external actor, the personal information involved in the incident is nonetheless sensitive and could be used for the purposes of identity theft and fraud. As well, the past operating practice of the malicious actor has been of locking up company systems, not in personal attacks of employees, however, the area of cyber attacks continues to evolve. The fact that the incident was caused as a result of the actions of an unknown actor with malicious intent additionally increases the likelihood that harm could result.* 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, ransom demand). The lack of evidence that the personal information has been misused is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach. Further, the information may have been available to the unauthorized third party for approximately two (2) weeks.

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, identity, financial and employment information at issue could be used to cause the significant harms of identity theft, fraud, financial loss and embarrassment. 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, ransom demand). The lack of evidence that the personal information has been misused is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach. Further, the information may have been available to the unauthorized third party for approximately two (2) weeks.

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 December 3, 2020 or by email on December 7, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner