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	Pomeroy Lodging LP (Organization)
Decision number (file number)	P2022-ND-043 (File #025406)
Date notice received by OIPC	April 1, 2022
Date Organization last provided information	May 5, 2022
Date of decision	June 27, 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 all or some of the following information: • name, • personal email address, • social insurance number, • personal cell phone number, and • physical address. 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 March 29, 2022, the Organization was alerted of a ransomware attack from one of its hotels. • The hackers had access to the Organization's servers that included payroll information for current and past staff.

	• The Organization's property management system and the credit card portals for client facing guests were not affected.
Affected individuals	The incident affected 2000 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• The Organization immediately moved to disaster recovery mode, which locked down its servers. • Continued cyber compliance and phishing email training. • Using a third party company to test its training on phishing emails and cyber security.
Steps taken to notify individuals of the incident	Affected individuals were notified by email sent on April 1, 2022.
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 that the possible harms that may occur as a result of the breach are, "*Unknown the information was within our payroll system, so may be nothing or may be used*." 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 the affected individuals' 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 that it was "*unsure*" of the likelihood that the harm will 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 Organization reported that the hackers did have access to its payroll 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 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 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 Organization reported that the hackers did have access to its payroll 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 email on April 1, 2022, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance