



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Welk Resort Group (Organization)
Decision number (file number)	P2019-ND-105 (File #012457)
Date notice received by OIPC	March 6, 2019
Date Organization last provided information	March 6, 2019
Date of decision	July 18, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
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”	<p>The incident involved the following information:</p> <ul style="list-style-type: none">• name,• address,• social security number, and• payment card information. <p>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.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• On or around August 2, 2018, the Organization learned of unusual activity related to an employee email account and immediately began an investigation to confirm the security of its network and determine the nature and scope of this event.

	<ul style="list-style-type: none"> The Organization learned that an unauthorized actor(s) was able to gain access to the employee's email account. Based upon available forensic evidence, the email account was subject to unauthorized access between July 24, 2018 and August 2, 2018.
Affected individuals	The breach affected eight (8) residents of Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> Immediately took steps to investigate, determine the nature and scope of the incident, as well as determine what data may potentially be affected. Worked with third-party forensic experts.
Steps taken to notify individuals of the incident	Affected individuals in Alberta were notified by mail beginning around February 22, 2019.
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 did not specifically identify potential harms that might result from this incident, but reported that it is "...providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud". In my view, a reasonable person would consider that the contact, identity and financial 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 did not specifically assess the likelihood of harm resulting from this incident, but reported its investigation "...found no evidence of actual or attempted misuse of personal information". In my view, a reasonable person would consider that the likelihood of harm resulting in this case is increased because the breach resulted from malicious intent (unauthorized access) and the information was exposed for over a week.
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 that the contact, identity and financial information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting in this case is increased because the breach resulted from malicious intent (unauthorized access) and the information was exposed for over a week.	

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 that individuals in Alberta were notified by mail beginning around February 22, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner