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	Rosewood Hotel Group (Organization)
Decision number (file number)	P2018-ND-015 (File #007539)
Date notice received by OIPC	January 19, 2018
Date Organization last provided information	January 19, 2018
Date of decision	January 26, 2018
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 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 information at issue includes: • name, and • payment card number, expiry date, security code. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's online Central Reservation System (CRS) used to process guest hotel reservations.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• In late December 2017, the Organization was notified by its third party service provider, Sabre Hospitality Solutions, that between May 29, 2016 and January 11, 2017, an unauthorized party had gained access to the Organization's guest reservation information that was maintained on Sabre's systems.

	• The Organization was informed that the unauthorized party gained access by obtaining account credentials from Sabre without authorization.
Affected individuals	The incident affected approximately 141 residents of Alberta.

Steps taken to reduce risk of harm to individuals	• Worked with the third party service provider to identify affected guests.
	• Reported that the third party service provider:
	  o took steps to disable impacted accounts and stop the unauthorized access to its systems.
	  o engaged an outside cybersecurity expert to conduct a forensic investigation.
	  o notified law enforcement and the relevant payment card brands of the issue.

Steps taken to notify individuals of the incident	Affected individuals were notified by mail or email beginning January 19, 2018. In addition, the Organization posted information about the incident on its website, including affected properties, dates of exposure and steps affected individuals can take to protect against misuse of personal information and identity theft.
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 it provided "recommendations on steps affected guests can take to help protect against misuse of their personal information and identity theft." In my view, the financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. 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 did not specifically assess the likelihood of harm occurring in this case. In my view, the likelihood of harm resulting from this incident is increased because the incident was the result of malicious intent (deliberate unauthorized intrusion) and the information was exposed for over seven months.

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. The financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm resulting from this incident is increased because the incident was the result of malicious intent (deliberate unauthorized intrusion) and the information was exposed for over seven months. I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand affected individuals were notified by mail or email beginning January 19, 2018. In addition, the Organization posted information about the incident on its website, including affected properties, dates of exposure and steps affected individuals can take to protect against misuse of personal information and identity theft. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner