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	New World Hotel Management Limited (d/b/a Rosewood Hotel Group) (Organization)
Decision number (file number)	P2017-ND-158 (File #006029)
Date notice received by OIPC	July 7, 2017
Date Organization last provided information	November 5, 2017
Date of decision	November 28, 2017
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 incident involved the following information: • name, • payment card number, expiry date, and possibly security code. In some cases, the following information is also at issue: • name, • email address, • telephone number, • address, • guest arrival and departure dates, • reservation status, and • other information associated with a reservation. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected through an online central reservations system.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On June 6, 2017, the Organization was notified by its service provider that an unauthorized party gained access to account credentials that permitted access to payment card data and certain reservation information for some hotel reservations processed through the service provider's Central Reservations System ("CRS"). • The unauthorized party was able to access payment card information for some hotel reservations at affected properties. The service provider's investigation found that the unauthorized party first obtained access to payment card and other reservation information on November 3, 2016. The last access to this information was on March 9, 2017.
Affected individuals	The incident affected three (3) Alberta residents.
Steps taken to reduce risk of harm to individuals	• The service provider has engaged a cybersecurity firm to support its investigation, and has notified law enforcement and payment card brands about the incident. • The service provider has taken measures to help ensure that the unauthorized access to the impacted systems was stopped. • Service provider has taken steps to enhance security and help prevent further unauthorized access to reservation records processed on its systems.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on or about July 7, 2017.
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 any harm that might result from this incident, but its notification to affected individuals stated "We recommend that you regularly review your account statements. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions." In my view, the contact, financial and profile information at issue could be used to cause the harms of identity theft and fraud. In addition, email address could be used to cause the harm of phishing. 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 did not specifically assess the likelihood of harm resulting from this incident but, as noted above, its notification to affected individuals stated "We recommend that you regularly review your account statements. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions." In my view, the likelihood of harm is increased because the incident was the result of malicious intent (deliberate intrusion) and the personal information was exposed for almost four (4) 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 contact, financial and profile information at issue could be used to cause the harms of identity theft and fraud. In addition, email address could be used to cause the harm of phishing. These are all significant harms. The likelihood of harm is increased because the incident was the result of malicious intent (deliberate intrusion) and the personal information was exposed for almost four (4) months.

I require the Organization to notify the affected individuals in Alberta accordance with section 19.1 of the Personal Information Protection Act Regulation (Regulation).

I understand the Organization notified the affected individuals by letter sent on or about July 7, 2017. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner