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	Four Seasons Hotels Limited (Organization)
Decision number (file number)	P2018-ND-28 (File #006027)
Date notice received by OIPC	July 7, 2017
Date Organization last provided information	July 7, 2017
Date of decision	February 16, 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)(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, and • other information association 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 processed through a central reservations system. To the extent that these transactions occurred in Alberta, I have jurisdiction in this matter.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On June 6, 2017, the Organization was notified by its service provider, Sabre Hospitality Solutions, 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 August 10, 2016. The last access to this information was on March 9, 2017.
Affected individuals	The Organization did not respond to correspondence sent from this office about how many Alberta residents were affected by the incident.
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 starting on July 6, 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 reported that, "This incident may result in financial loss to affected individuals, although the potential harm is mitigated by the fact that individual liability for fraudulent charges to credit cards that are timely reported is limited." In my view, the contact, financial and profile information at issue could be used to cause the harms of identity theft, financial loss, and fraud. In addition, email addresses 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 reported that it "does not believe that the potential harm is significant…this incident did not affect every reservation contained in the CRS, but only a smaller subset of reservations… (the) investigation did not uncover specific forensic evidence that the unauthorized party removed any information from the system, but it is a possibility… (the) Organization has not received any reports of identity fraud, theft or specific misuse of information as a direct result of the incident." 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 seven (7) months. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud, which can occur many months or even years after an incident.

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, financial loss, and fraud. In addition, email addresses 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 seven (7) months. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud, which can occur many months or even years after an incident.

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 the Organization notified the affected individuals by letter commencing on July 6, 2017. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner