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-61 (File #007687)
Date notice received by OIPC	February 1, 2018
Date Organization last provided information	March 8, 2018
Date of decision	June 18, 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 incident involved all or some of the following information: • name, • email address, • telephone number, • address, and • payment card number, expiry date and potentially 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 online Central Reservation System (CRS) of the Organization's third party reservation service provider, Sabre Hospitality Solutions.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On December 15, 2017, the Organization was notified by its third party reservation service provider, Sabre Hospitality Solutions, that an unauthorized party gained access to view certain reservation information on October 21, 2017. • The service provider informed the Organization that it uses encryption on payment card data; however, the compromised credential had the right to decrypt card data. • The service provider informed the Organization that the incident did not affect every reservation contained in the CRS, but only a smaller subset of reservations. • The service provider reported that its investigation did not uncover specific forensic evidence that the unauthorized party removed any information from the system, but it is a possibility.
Affected individuals	The incident affected 25 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Successful measures were taken by the service provider to ensure that the unauthorized access to the CRS was stopped. • Instituted a call centre to field any questions or concerns from affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail or email on January 15, 2018. The Organization also posted a notice on the websites of the two impacted hotels and filed a press release with PR Newswire.
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 "This incident may result in financial loss to affected individuals, although that potential harm is mitigated by the fact that individual liability for fraudulent charges to credit cards that are timely reported is limited." I agree with the Organization that the financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. These are significant harms. The contact information at issue, as well as email address, could be used for unsolicited telephone calls, emails and phishing. I have previously found phishing to be a significant harm.
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 its service provider reported that "…unencrypted payment card data and reservation information was available for a brief period on October 21, 2017…this incident did not affect every reservation contained in the [CRS], but only a smaller subset of reservations… [the service provider's] 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 this incident. Given these factors, there is a low risk that harm could result." 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). Further, the lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing or identity theft and fraud can occur months and years after a data breach. The Organization can only speculate that affected individuals may 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.

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 harms of identity theft, fraud and financial loss. These are significant harms. The contact information at issue, as well as email address, could be used for unsolicited telephone calls, emails and phishing. I have previously found phishing to be a significant harm. The likelihood of harm resulting from this incident is increased because the incident was the result of malicious intent (deliberate unauthorized intrusion). Further, the lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing or identity theft and fraud can occur months and years after a data breach.

The Organization can only speculate that affected individuals may 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.

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 affected individuals by mail or email on January 15, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner