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	Six Continents Hotels, Inc., a franchisee of Intercontinental Hotels Group Company (Organization)
Decision number (file number)	P2017-ND-157 (File #005444)
Date notice received by OIPC	April 18, 2017
Date Organization last provided information	November 22, 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 all or some of the following information: • name, and • payment card number, expiration date and internal verification code. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from cards used onsite at the front desk of certain Organization-branded franchise hotel locations. To the extent these transactions occurred in Alberta, I have jurisdiction in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• In January 2017, several franchisees were made aware by payment card networks of patterns of unauthorized charges occurring on payment cards after they were legitimately used at franchise locations. The franchisees reported this information to Intercontinental Hotels Group Company (IHG).

	• IHG coordinated an examination of the payment card processing systems of franchise hotel locations in the Americas. • The investigation found signs of the operation of malware designed to access payment card data from cards used onsite at certain hotel locations between September 29, 2016 and December 29, 2016. • Before the incident, many franchise hotel locations implemented IHG's Secure Payment Solution (SPS), a point-to-point encryption payment acceptance solution. Properties that implemented the solution before September 29, 2016 were not affected by this incident. Those properties that implemented SPS after September 29, 2016 ended the ability of the malware to find payment card data and therefore cards used at these locations after SPS implementation were not affected.
Affected individuals	The incident affected 28,809 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Hired a cyber security firm on behalf of franchisees to coordinate the examination of the payment card processing systems. • Established a dedicated call centre that affected individuals can contact with questions. • Recommended that individuals remain vigilant to the possibility of fraud. • Confirmed that malware was eradicated. • Evaluated ways for franchisees to ensure security measures. • Notified law enforcement.
Steps taken to notify individuals of the incident	On behalf of franchisees, the Organization notified affected individuals by letter starting on April 14, 2017 and provided substitute notification on April 18, 2017 by posting a statement on its website and issuing a news release.
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 the possible harm that might result from this incident include the information being used to make "fraudulent purchases elsewhere online. However, generally card network regulations provide that cardholders are not responsible for fraudulent charges that are timely reported to the issuer of the card." In my view, the identity and financial information at issue (including payment card numbers, security codes and expiry dates) 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 reported that "Given that in Canada there is zero liability for fraudulent credit card purchases made on an individuals' credit card, there is no risk of significant harm to the affected individuals in Alberta arising from this incident. The affected individuals will be made whole by their credit card issuer. There may be inconvenience associated with the replacement cars, but that is not a significant harm." In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and installation of malware). Further, the information may have been exposed for approximately three 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.

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 identity and financial information at issue (including payment card numbers, security codes and expiry dates) could be used to cause the harms of identity theft, fraud and financial loss. These are significant harms. In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and installation of malware). Further, the information may have been exposed for approximately three 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.

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 in a letter starting on April 14, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner