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	Aimbridge Hospitality Holdings, LLC (Organization)
Decision number (file number)	P2017-ND-142 (File #006572)
Date notice received by OIPC	September 12, 2017
Date Organization last provided information	October 12, 2017
Date of decision	November 6, 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 the 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 may have involved the following information: • name, • payment card number, expiry date, and security code. In some cases, the following information may also be at issue: • name, • email address, • telephone number, • address, 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 processed through a central reservations system. The Organization reported that approximately 41 residents of Alberta may have been affected by this incident.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization manages a number of hotel properties. • On June 6, 2017, the Organization was notified by its service provider that an unauthorized party obtained access to account credentials that permitted unauthorized access to unencrypted payment card information as well as certain reservation information for a subset of hotel reservations processed through the service provider's central reservation system ("CRS"). • The incident was discovered by the service provider on or about March 10, 2017. • Access to payment card and other reservation information occurred between August 10, 2016 and March 9, 2017. • Multiple hotels were impacted by this incident.
Affected individuals	The incident may have affected forty-one (41) Albertans.
Steps taken to reduce risk of harm to individuals	• Forensic experts investigated the incident. • Law enforcement was notified as well as payment card brands. • The Organization published a notice of the incident on the homepages of the affected hotels. This notice was published beginning on or about July 6, 2017. • Notification was provided to impacted individuals. The notification included information on ways to protect against the misuse of personal information including information on credit reports, fraud alerts and security freezes. • On August 24, 2017, the Organization issued a nationwide press release regarding the incident. • The service provider purchased additional security controls to better secure their accounts and protect the data. They have also enhanced their monitoring practices. • The Organization is taking additional steps going forward to work with service providers to better protect the privacy and security of the Organization's data. The Organization "continues to work to improve its own security posture as well".
Steps taken to notify individuals of the incident	The Organization notified affected individuals directly by mail on August 24, 2017 or by email on August 25, 2017. Notice was also posted on the hotels' websites on or about July 6, 2017. A press release went out on August 24, 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 reported it was "providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file …[and] a reminder to remain vigilant for incidents of fraud and identity theft". 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, reported it was "providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file …[and] a reminder to remain vigilant for incidents of fraud and identity theft". 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.

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 seven (7) months.

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

The Organization notified the affected individuals directly by mail on August 24, 2017 or by email on August 25, 2017. Notice was also posted on the hotels websites on or about July 6, 2017. A press release went out on August 24, 2017. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner