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	Hersha Hospitality Management LP (Hersha) and the Marriott Courtyard (Courtyard) (collectively, "the Organizations")
Decision number (file number)	P2016-ND-19 (File #001296)
Date notice received by OIPC	July 17, 2015
Date Organization last provided information	February 24, 2016
Date of decision	June 2, 2016
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organizations are 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 Organizations are "organizations" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following information is at issue for the one Alberta resident affected by this incident: • name, • payment card information (including account type, account • number and expiration date). This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
☒ loss ☐ unauthorized access ☐ unauthorized disclosure	

Description of incident	• Hersha manages the Courtyard in San Diego, California. • On May 6, 2015, the Courtyard discovered an office used by Courtyard sales associates had been burglarized. • Paper files containing guest and employee personal information were stolen. • The Courtyard discovered the theft and promptly reported it to the San Diego Police Department. • To date, the paper files have not been recovered and there have been no arrests made.
Affected individuals	One (1) Albertan was affected by this incident.
Steps taken to reduce risk of harm to individuals	• The Organizations initiated an investigation. • Safety deposit boxes will be used to store printed payment card information. • Additional locks installed on sales and accounting offices. • The Organizations provided affected individuals with information about protecting themselves against identity theft and fraud.
Steps taken to notify individuals of the incident	Notified in writing on September 15, 2015.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 the type of harm that might result from this breach includes "misuse of the information to perpetuate fraud or identity theft". I agree with the Organization's assessment. The personal information involved includes financial information that could be used to cause the harms of identity theft and fraud. 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 Organizations reported this breach "did not present a real risk of significant harm … as Hersha was and remains unaware of any actual or attempted misuse of the information. Nevertheless, Hersha determined that the possibility of actual or attempted misuse of the Alberta resident's information cannot be completely ruled out, as the paper files have not been recovered."

	In considering the likelihood of harm resulting from the incident, the Organizations considered: • The identity of the burglar is unknown. Therefore, it is unknown whether there is a relationship between the burglar and the data subjects, or the burglar and the Organizations. • The Organizations are not currently aware of any actual or attempted harm to affected individuals. • There is no evidence of fraud or misuse of the information at this time. In my view, the likelihood of harm resulting from this incident is increased because the personal information was stolen, The perpetrator has not been apprehended, and the personal information has not been recovered.

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 individual. The personal information involved includes sensitive financial information that could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased because the personal information was stolen, indicating malicious intent. The perpetrator has not been apprehended, and the personal information has not been recovered.

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

I understand the Organization notified the affected individual on September 15, 2015. The Organization is, therefore, not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner