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	Magellan Vacations (operating as Magellan Luxury Hotels) (Organization)
Decision number (file number)	P2017-ND-108 (File #005996)
Date notice received by OIPC	June 27, 2017
Date Organization last provided information	July 11, 2017
Date of decision	August 4, 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)(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 if provided to the hospitality central reservations system. 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.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization uses a central reservations system (CRS) provided by a third party service provider. • The Organization received information from the service provider that an unauthorized party obtained access to account credentials that permitted access to a subset of hotel reservations processed through the hospitality CRS. • The unauthorized party used the account credentials to view a credit card summary page on the hospitality CRS and to access payment card information. • The unauthorized access first occurred on August 10, 2016. The last access to payment card information was on March 9, 2017.
Affected individuals	The incident affected 1,766 clients, including 13 individuals from Alberta.
Steps taken to reduce risk of harm to individuals	The Organization reported its service provider said "We took successful measures to ensure this unauthorized access to the Hospitality CRS was stopped and is no longer possible. Our investigation did not uncover forensic evidence that the unauthorized party removed any information from the system, but it is a possibility. We notified law enforcement and the payment card brands, and we engaged a PCI Forensic Investigator to investigate this incident. "
Steps taken to notify individuals of the incident	The Organization notified affected individuals by email sent June 27, 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 "Primary issue is the exposure of credit card information, which could result in financial consequences to the clients if this leads to fraud." Further, "The disclosure of credit card information can have negative effects on customers if the cards are used for fradulent [sic] activity." In my view, the contact, financial and profile information (i.e. reservations) 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.	In its report, the Organization noted that the incident occurred over "a six month period" and "To access this quantity of information for this long, can only suggest that the indended [sic] purpose was for fraudulent purposes." The Organization also noted that some affected individuals could be seniors. 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 (i.e. reservations) 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 Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by email sent June 27, 2017. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner