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	Hyatt Hotels Corporation (Organization)
Decision number (file number)	P2017-ND-05 (File #002214)
Date notice received by OIPC	January 18, 2016
Date Organization last provided information	June 17, 2016
Date of decision	January 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 registered as an extra provincial corporation and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	Some or all of the following information was involved in this incident: • name, • credit card number, expiry date, and security code (CVV). This information is about identifiable individuals 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	• On November 30, 2015, the Organization confirmed the presence of malware designed to target payment card data. • The Organization investigated and hired third party security experts to examine its payment card network.

	• The investigation indicated potential unauthorized access to payment card information from cards used at certain managed locations or provided to a sales office between August 13, 2015 and December 8, 2015, as well as on or shortly after July 30, 2015 for a limited number of cards. • On January 18, 2016 the Organization's call center was contacted by an individual who reported 2 fraudulent payment card charges. • The perpetrator(s) responsible for the incident have not been identified nor arrested.
Affected individuals	The total number of individuals affected is unknown; however, one (1) resident of Alberta reported two (2) fraudulent charges on a payment card.
Steps taken to reduce risk of harm to individuals	• Reported the incident to the Federal Bureau of Investigation and U.S. Secret Service. • Cooperating with payment card providers to identify the cards potentially at risk. • Implemented containment and security enhancement measures, including removal of the malware. • Encouraging customers to monitor accounts and report unauthorized charges.
Steps taken to notify individuals of the incident	• On December 23, 2015, the Organization issued a preliminary statement concerning its ongoing investigation, posting a notice on its website and issuing a press release. • The Organization posted a list of affected locations along with the potential at-risk time frames on its website. • On January 14, 2016, the Organization published a substitute notice on its website and issued a press release. • Notified affected individuals (for whom the Organization had contact details) by letter or email on January 19, 2016. This included 7 Albertans.
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 "Stolen payment card information is generally used to make counterfeit cards that are then used to make fraudulent charges." I agree with the Organization's assessment. The information at issue 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 Organization reported that "potential harm is not likely to be significant" because "card networks generally have operating regulations that provide that cardholders are not responsible for fraudulent charges that are timely reported to the bank who issued the card." In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and malware) and the information was potentially exposed for almost 5 months before the incident was discovered. The Organization has received at least one report of fraudulent credit card charges that may be the result of this incident and the Organization can only speculate that affected individuals will not be held responsible for fraudulent credit card purchases. 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 as a result of this incident. The information at issue could be used to cause the significant harms of identity theft and fraud. The breach was the result of malicious intent (deliberate intrusion and malware) and the information was potentially exposed for almost 5 months before the incident was discovered. The Organization has received at least one report of fraudulent credit card charges that may be the result of this incident and the Organization can only speculate that affected individuals will not be held responsible for fraudulent credit card purchases. 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 on January 14, 2016, the Organization published a notice of this incident on its website and issued a press release. On January 19, 2016, the Organization notified affected individuals directly by letter or email, where contact details were available. Where the Organization does not have valid contact information for affected individuals, I am satisfied that substitute notice (via the Organization's website and press release) is reasonable in the circumstances. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner