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	Noble House Hotels and Resorts (Organization)
Decision number (file number)	P2017-ND-144 (File #006264)
Date notice received by OIPC	August 8, 2017
Date Organization last provided information	October 20, 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 those individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates hotels and resorts in the United States and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved some or all of the following information: • name, and • payment card number, expiry date and security code. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported "Alberta residents could have made reservations directly through the hotels websites or through a 3rd party site".
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization initiated an investigation when it was notified by the Secret Service about possible fraudulent activity on the payment card system at one of the Organization's properties.

	• The Organization discovered that malware may have been installed on payment processing systems that potentially affected payment cards of individuals that were swiped at some of its hotels, restaurants and bars between April 25, 2016 and August 5, 2016.
Affected individuals	The incident affected 24 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Engaged a computer security firm to examine the payment system at all of its properties for any signs of an issue. • Established a dedicated call centre to assist individuals with any questions regarding the incident. • Worked with a computer firm to ensure that the malware issue was fully remediated. • Reviewed and enhanced its security measures.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter beginning on September 2, 2016. The Organization also posted a statement on the home page of its website and by issuing a press 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.	In its report of the incident, the Organization did not specifically identify harms that could result from the incident. However, the Organization's notice to affected individuals recommended they "remain vigilant to the possibility of fraud and identity theft…". In my view, the financial information at issue could be used to cause the significant harms of fraud, financial loss and identity theft.
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 of the incident, the Organization did not specify the likelihood that harm to affected individuals could result. 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 appears to have been exposed for approximately 3.5 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 financial information at issue could be used to cause the significant harms of fraud, financial loss and identity theft. 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 appears to have been exposed for approximately 3.5 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 letter beginning on September 2, 2016 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner