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-94 (File #001732)
Date notice received by OIPC	November 17, 2015
Date Organization last provided information	May 30, 2017
Date of decision	July 17, 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 the following information: • name, and • credit 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 information was collected from residents of Alberta through the Organization's website, by phone, or in-person.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization began investigating when some of its guests noticed unauthorized charges appeared on their payment cards used at the Organization's properties.

	• On September 25, 2015, the Organization learned that malware may have been installed on payment processing systems that potentially affected payment cards swiped at certain properties between December 29, 2014 and August 11, 2015.
Affected individuals	The incident affected 157 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Discovered and removed the malware. • Notified the FBI regarding the incident. • Engaged a computer security firm to examine its payment processing system. • Established a dedicated call center to assist affected individuals with any questions regarding the incident. • Took action to strengthen and enhance the security of its system. • Reviewed practices, policies, and procedures. • Implemented enhanced measures to prevent future occurrences.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter beginning on November 13, 2015. The Organization also posted a statement on each affected property's website, and a press release was issued through a public relations newswire that described the incident.
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. However, the Organization reported that it has "seen a few instances of fraudulent activity." 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) and the Organization has seen a few instances of fraudulent activity. Further, the information may have been exposed for up to 8 (eight) 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) and the Organization has seen a few instances of fraudulent activity. Further, the information may have been exposed for up to 8 (eight) 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 November 13, 2015 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner