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	Best Western Plus Wine Country Hotel & Suites in West Kelowna, operated by 626498 Alberta Ltd. (Organization)
Decision number (file number)	P2017-ND-130 (File #006426)
Date notice received by OIPC	September 5, 2017
Date Organization last provided information	September 5, 2017
Date of decision	September 11, 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 following information may have been involved in this incident: • first and last name, • address, • telephone number and email address, • credit card number and expiry date, and • credit card magnetic stripe information and credit card CVV or CVC numbers for individuals who swiped their credit cards to confirm their booking. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta (e.g. via the Organization's website), I have jurisdiction in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On September 17, 2016, a reservation clerk with the Organization unknowingly opened a phishing email which caused malware to be downloaded onto the Organization's front desk system. • On November 20, 2016, the Organization's Head Office advised that there may have been possible fraudulent activity linked to one or more of the Organization's hotels, and requested investigations. The Organization engaged a computer forensics expert but no breach was discovered. • On May 4 and 19, 2017, two different credit card brands notified the Organization's that fraudulent activity was detected. The same computer forensics expert was called in to investigate, and on May 25, 2017, the expert again advised that no breach was discovered. • The Organization sought a second opinion from a different computer forensic expert, and on July 20, 2017, learned that a breach had occurred on September 17, 2016 via the phishing email. • The breach was contained and malware removed on July 20, 2017.
Affected individuals	The incident affected approximately 5,423 individuals, including 1,100 guests from Alberta.
Steps taken to reduce risk of harm to individuals	• Identified malware and blocked it from executing. Scanning other systems to ensure malware did not spread. • Notified payment card brands, who cancelled the credit cards and re-issued new cards. • Completely wiped and rebuilt the front desk system, and converted the reservation system to be operated offline. • Strengthening computer security to all systems. • Setting up a dedicated front desk system for email reservations with enhanced security protections. • Notified law enforcement and privacy commissioners in BC and Quebec, as well as the federal commissioner. • Retaining IT firm to conduct ongoing vulnerability assessments and provide security services to all systems. Also retaining a third party IT company to provide services.
Steps taken to notify individuals of the incident	The Organization reported that it decided to notify all guests that stayed at the hotel and were in its records between September 1, 2016 to July 20, 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 identified "fraud or identity theft" and the "potential for phishing scams" as harms that might result from this incident. In my view, the contact and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. Email address could be used to cause the harm of phishing. 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 it "do[es] not think there is a real risk of significant harm". Specifically, "There is a low risk of individuals suffering fraud or identity theft because the credit card numbers accessed have been cancelled, and new cards reissued. We do not know if any of the card numbers accessed were fraudulently used before they were cancelled. There may also be potential for phishing scams, although it's uncertain whether any email addresses were actually accessed or misused by the unauthorized party." In my view, the likelihood of harm is increased because the incident was the result of malicious intent (deliberate intrusion and installation of malware) and the personal information was exposed for approximately 10 months. The Organization investigated and discovered the incident after reports of possible fraudulent activity.

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 and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. Email address could be used to cause the harm of phishing. These are significant harms. The likelihood of harm is increased because the incident was the result of malicious intent (deliberate intrusion and installation of malware) and the personal information was exposed for approximately 10 months. The Organization investigated and discovered the incident after reports of possible fraudulent activity.

I require the Organization to notify the affected individuals in Alberta accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). The Organization reported that it decided to notify all guests that stayed at the hotel and were in its records between September 1, 2016 to July 20, 2017. **I require the Organization to confirm to me, within 10 days of the date of this decision, that affected individuals in Alberta were notified in accordance with the Regulation.**

Jill Clayton
Information and Privacy Commissioner