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	Hilton Worldwide Inc. (Organization)
Decision number (file number)	P2017-ND-84 (File #001986)
Date notice received by OIPC	December 11, 2015
Date Organization last provided information	May 7, 2017
Date of decision	June 20, 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, • payment card information (payment card number, security code, and expiration date), and • primary account numbers, or PANs (a subset of PANs were found in combination with name only). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, I have jurisdiction in this matter.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On February 10, 2015, the Organization was notified by a service provider of potential malware activity targeting its payment card systems on a server.

	• The Organization initiated an investigation and hired a third party forensic investigator. • The investigation revealed 2 malware output files containing payment card information on an Organization server. The malware targeted the systems between November 18, 2014 and December 5, 2014. • The forensic investigator concluded that there was no direct evidence that payment card information was removed. • On November 19, 2015, the Organization was notified by a payment card company that potentially fraudulent activity had been noted with respect to payment cards used at Organization properties between February 10 and November 19, 2015. • The Organization has not identified any complaints as a result of the incident affecting Canadian individuals.
Affected individuals	• The Organization reported the total number of affected individuals cannot be determined. Payment card information is not maintained or associated with individual contact information. • However, the investigation revealed the malware output files contained payment card information for approximately 26,347 individuals. • The Organization notified 564 Albertans of this and another incident. The Organization had the email contact information for these individuals.
Steps taken to reduce risk of harm to individuals	• Notified payment card companies and banks. • Reported to United States federal law enforcement. • Implemented containment and enhanced security measures, including the removal of the malware. • Offered one year of free credit monitoring.
Steps taken to notify individuals of the incident	• On November 24, 2015, the Organization published a notice regarding this and another incident on its webpage and via major media outlets. • The Organization issued a public statement via Business Wire Global Media Outlets, which included Canadian media coverage. • On December 8, 2015, the Organization provided notice by email to potentially affected individuals if it had email contact information for the individuals. This included 564 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 stated that if payment card information had been removed or stolen, the data could be used for fraudulent transactions. The Organization stated that "it understands that the Alberta OIPC has previously identified such data as sensitive." In my view, the financial 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 its investigation "to date indicates no exfiltration of payment card data has occurred. Further, the payment card companies were notified … of the potentially affected payment cards. Finally, the major card networks have systems in place designed to detect payment card fraud and consumers generally receive refunds from payment card companies for fraudulent charges that the consumers see on their payment card accounts and report to their payment card companies. Accordingly, the actual risk of significant harm to an individual payment card holder appears relatively low at this point." In my view, the likelihood of harm resulting from this incident is increased as it was the result of malicious intent and the presence of third party malware. The malware was operational for approximately 3 weeks and was not discovered for some time. Although the Organization reported there is no evidence the information at issue was removed, this cannot be known for sure. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud. Finally, I note that harm may have been realized as the payment card company notified the Organization in November 2015 that potentially fraudulent transactions had been noted at the Organization's properties.

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 financial information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm is increased as the incident was the result of malicious intent and the presence of third party malware. The malware was operational for approximately 3 weeks and was not discovered for some time. Although the Organization reported there is no evidence the information at issue was removed, this cannot be known for sure.

The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

Finally, I note that harm may have been realized as the payment card company notified the Organization in November 2015 that potentially fraudulent transactions had been noted at the Organization's properties.

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 posted a general public notice of both incidents on its webpage and through major media outlets on November 24, 2015. The Organization directly notified affected individuals on December 8, 2015, where an email address was available, including 564 Albertans.

Where the Organization does not have contact information for affected individuals, I am satisfied that substitute notice on the Organization's website and media releases was reasonable in the circumstances. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner