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	Roberts Hawaii, Inc. (Organization)
Decision number (file number)	P2018-ND-082 (File #005088)
Date notice received by OIPC	February 27, 2017
Date Organization last provided information	February 27, 2017
Date of decision	July 16, 2018
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 in Alberta 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 incident involved all or some of the following information about the individuals: • name, • address, • email address, • telephone number, • 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 information was collected in Alberta via the Organization's websites (robertshawaii.com, and airportwaikikishuttle.com).
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization received reports from several customers of fraudulent charges appearing on their payment cards shortly after they were used to make a purchase on the Organization's website. • The Organization engaged a cybersecurity firm to investigate. The investigation determined that an unauthorized person gained access to the web server for two of the Organization's websites and installed code that was designed to copy information entered during the checkout process. • Information from purchases made between July 30, 2015 and December 14, 2016.
Affected individuals	The incident affected 565 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged a cybersecurity firm to investigate. • Removed the malware, and is taking steps to further strengthen the security of its website to help prevent a similar incident from happening in the future. • Reported the incident to law enforcement. • Established a dedicated call center to respond to affected individuals. • Recommending that potentially affected individuals remain vigilant to the possibility of fraud by reviewing their account statements and credit reports for unauthorized activity.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter sent February 24, 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 reported that "The order information affected here includes payment card information which is generally used to make fraudulent purchases elsewhere online. However, generally card network regulations provide that cardholders are not responsible for fraudulent charges that are timely reported to the issuer of the card." In my view, the contact and financial (payment card) information involved could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing purposes, which I have previously said is a significant harm.

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 it "… is taking steps to reduce the potential impact of this incident on its customers… has stopped the incident, removed the unauthorized code, and is taking steps to further strengthen the security of its websites to help prevent a similar incident from happening in the future. [The Organization] is recommending that potentially affected individuals remain vigilant to the possibility of fraud by reviewing their account statements and credit reports for unauthorized activity. [The Organization] has also established a dedicated call center that potentially affected individuals can contact with questions." In my view, the likelihood of harm resulting from this incident is increased because the incident was the result of malicious intent (deliberate intrusion and installation of malware), and the information was exposed for over 16 months. The Organization can only speculate that affected individuals will not be held responsible for fraudulent credit card purchases, and does not have any control over this remedy. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud, or the already noted possible use of the information for phishing purposes.

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 (payment card) information involved could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing purposes, which I have previously said is a significant harm.

The likelihood of harm resulting from this incident is increased because the incident was the result of malicious intent (deliberate intrusion and installation of malware), and the information was exposed for over 16 months. The Organization can only speculate that affected individuals will not be held responsible for fraudulent credit card purchases, and does not have any control over this remedy. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud, or the already noted possible use of the information for phishing purposes.

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 the affected individuals in a letter dated February 24, 2017, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner