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	EMC Business Solutions LLP (Organization)
Decision number (file number)	P2019-ND-173 (File #013427)
Date notice received by OIPC	June 19, 2019
Date Organization last provided information	June 19, 2019
Date of decision	November 26, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individuals whose personal information was collected 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) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved a keylogger installed on the Organization's website from January 10 - February 23, 2019. The following information could have been captured by the keylogger: • full name, • address, • email, • username password for the website, • credit card information, • telephone number, and • potentially employer/company name. 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 ecommerce website, store.beachcomberhottubs.com.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On February 23, 2019, the Organization learned that it was the victim of a malware attack on its ecommerce website. • An investigation determined that a keylogger was installed from January 10 to February 23, 2019. During this period, the keylogger had the ability to capture all keystrokes entered by individuals completing a transaction on the website. • The incident was discovered on February 21, 2019, when the Organization's IT discovered evidence of a malicious URL. The Organization continued to monitor the website and on February 23, 2019, discovered the keylogger.
Affected individuals	The incident affected 125 Canadians, including 17 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Removed the keylogger within hours of detection. • Took steps to upgrade the ecommerce platform and applied an additional security patch. • Continuing to monitor network activity on the server to detect any suspicious activity. • Offered affected individuals one year of free credit and identity theft monitoring. • Advised all individuals who completed their transaction through a registered account to change their passwords on any accounts where they may have used the same password. • Reported the breach to the Office of the Information and Privacy Commissioner of British Columbia and the Office of the Privacy Commissioner of Canada.
Steps taken to notify individuals of the incident	Affected individuals were notified on March 15, 2019 and April 23, 2019 by email and mail.
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 "The possible harms could include financial fraud, identity theft, and phishing campaigns." In my view, a reasonable person would consider that the financial information at issue could be used to cause the harms of identity theft and fraud. Credentials could be used to compromise other online accounts. Email addresses could be used for phishing purposes, increasing vulnerability to 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 "There is a reasonable likelihood that harm may result because this was an intentional and malicious attack on [the Organization's] Website perpetrated by threat actors who may have gained access to personal information as a result of the Keylogger recording personal information as …customers were in the course of completing a transaction on the Website." The Organization also said that it "…does not have any information to suggest or confirm that the keystrokes and information captured by the Keylogger has been used by the unauthorized party who installed the Keylogger in any way…". In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach appears to be the result of malicious intent (deliberate action and installation of malware). The information was exposed for over a month.

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.

A reasonable person would consider that the financial information at issue could be used to cause the harms of identity theft and fraud. Credentials could be used to compromise other online accounts. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident is increased as the breach appears to be the result of malicious intent (deliberate action and installation of malware). The information was exposed for over a month.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand affected individuals were notified on March 15, 2019 and April 23, 2019 by email and mail. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner