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	Plant Therapy, Inc. (Organization)
Decision number (file number)	P2018-ND-145 (File #010060)
Date notice received by OIPC	October 19, 2018
Date Organization last provided information	October 19, 2018
Date of decision	November 15, 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 whose 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's principal address is in Idaho, USA. 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 may have involved the following information: • name, • address, • user name and password for the Organization's website, and • payment card information, including 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 via the Organization's ecommerce website, www.planttherapy.com.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On May 11, 2018, the Organization learned of a potential data security incident involving the unauthorized installation of malware on the ecommerce web platform of its third-party provider. • The malware created an iframe overlay designed to capture billing details entered by the customer during the shopping cart checkout process. • The incident potentially exposed the payment card information of individuals who made purchases on the ecommerce website between March 29 and May 11, 2018. • On July 20, 2018, ongoing monitoring efforts revealed additional individuals may have been affected by the incident. These additional individuals may include customers who used the ecommerce platform between July 17- 20, 2018, and whose information may have been accessed following the reinstallation of malware on its third party provider's ecommerce web platform. • The personal information of one Alberta resident may have been affected twice during the ongoing data incident.
Affected individuals	The incident may have affected 502 Canadian residents, including 66 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Took steps to secure customer payment card information. • Launched an investigation and worked with a forensics firm to remove malicious code from the third-party ecommerce web platform and to block traffic to *I* from malicious domains. • Retained a second forensics firm to investigate the ongoing incident, remediate, and determine the number of affected individuals and the personal information involved. • Took steps to require increased security from the third-party ecommerce platform. • Reported the breach to the United States Federal Bureau of Investigation, appropriate Data Protection Authorities, and the applicable payment card brands. • Offered complimentary identity monitoring services for 24 months.
Steps taken to notify individuals of the incident	Affected Canadians were notified on July 13, 2018, and again on September 12, 2018. The Alberta resident who may have been affected on two occasions received a follow-up letter on July 12, 2018.

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 it "…provided affected Canadians with a resource guide, which includes information and resources on how they can protect themselves from, or address issues of fraud or identity theft." In my view, a reasonable person would consider the contact, credentials and financial information at issue could be used to cause the significant harms of identity theft and fraud.
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 did not specifically assess the likelihood of harm resulting from this incident, but reported that it "…is of the view that the test for mandatory breach reporting under the *Personal Information Protection Act* (Alberta) is met and that individual notification is also required (as well as being the right thing to do)." 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 (installation of malware). It is not clear from the Organization's report how long the information may have been exposed.

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 the contact, credentials and financial information at issue could be used to cause the significant harms of identity theft and fraud. 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 (installation of malware). It is not clear from the Organization's report how long the information may have been exposed.

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 Canadians were notified on July 13, 2018, and again on September 12, 2018. The Alberta resident who may have been affected on two occasions received a follow-up letter on July 12, 2018. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner