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	Safe for Home Products LLC d/b/a/ Naturepedic (Organization)
Decision number (file number)	P2017-ND-45 (File #004652)
Date notice received by OIPC	January 3, 2017
Date Organization last provided information	January 3, 2017
Date of decision	March 8, 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 was involved in this incident: • name, • address, • telephone number, • credit card information. 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.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On October 28, 2016, "during an extensive scan", the Organization learned that encrypted malware was placed on its www.naturepedic.com website. • The malware copied information entered to the website to create online accounts used to place orders between June 6 and October 28, 2016.

Affected individuals	A total of 8 residents of Alberta were affected.
Steps taken to reduce risk of harm to individuals	• Worked with third party website service provider to identify and remove the malware and to implement additional safeguards. • Reported incident to law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified in writing on December 28, 2016.
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 reported the possible harm that might result from this incident to be "credit cards being used fraudulently." I agree with the Organization's assessment. Financial information (credit card information) could be used to cause fraud and financial loss, as well as identity theft. 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 "We are mitigating any potential harm by providing one year of free credit monitoring and $1 million of identity theft insurance." In my view, the likelihood of harm resulting from this breach is increased because the incident resulted from malicious intent (deliberate intrusion and installation of malware), the information was exposed for over four months, and it was used to set up fraudulent accounts and to place orders. I appreciate the Organization's efforts to mitigate possible harm through credit monitoring and identity theft insurance; however, affected individuals must contact the service provider, enroll and activate these services themselves using information provided by the Organization, which they can only do if they have been notified of the risk of harm.

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.

Financial information (credit card information) could be used to cause fraud and financial loss, as well as identity theft. These are significant harms. The likelihood of harm resulting from this breach is increased because the incident resulted from malicious intent (deliberate intrusion and installation of malware), the information was exposed for over four months, and it was used to set up fraudulent accounts and to place orders. I appreciate the Organization's efforts to mitigate possible harm through credit monitoring and identity theft insurance; however, affected individuals must contact the service provider, enroll and activate these services themselves using information provided by the Organization, which they can only do if they have been notified of the risk of harm.

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 affected individuals in writing on December 28, 2016. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner