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	AeroGrow International Inc. (Organization)
Decision number (file number)	P2017-ND-54 (File #000959)
Date notice received by OIPC	June 10, 2015
Date Organization last provided information	July 10, 2015
Date of decision	May 19, 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"	I have jurisdiction because 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 the following information: • name, • address, • credit and debit card number, expiration date, and CCV/CVV 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 website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization was alerted that some of its customers had experienced credit card fraud. • The Organization investigated and found there had been unauthorized access to its website. • The Organization discovered the incident on May 5, 2015. Malware that had been installed was removed.

	• On June 10, 2015, the Organization discovered and removed additional malware from the website. • The Organization reported that the website may have been compromised between October 15, 2014 and April 27, 2015 as well as between May 13, 2015 and June 10, 2015. • The Organization reported that although the investigation did not find evidence that customer information was removed from the website, "it seems likely that they extracted at least some customer information."
Affected individuals	The Organization reported that 436 individuals in Alberta who entered their personal information into the Organization's website between October 15, 2014 and April 27, 2015 were potentially affected by the incident. An additional 18 individuals in Alberta were potentially affected during the second attack.
Steps taken to reduce risk of harm to individuals	• A cybersecurity firm was hired to conduct an investigation into the incident. The malicious software codes were removed from the website. • A comprehensive review of the system security was conducted and steps were taken to prevent re-occurrence of the incident. • The incident was reported to law enforcement. • General advice on how to protect personal information was provided to customers. • Affected individuals were provided with the contact information of someone who could respond to questions about the incident.
Steps taken to notify individuals of the incident	The Organization notified affected individuals in writing on July 10, 2015.
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 thieves could potentially use the affected customers' credit card information to commit credit card fraud." I agree with the Organization's assessment. 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.	In assessing the likelihood of harm resulting from this incident, the Organization noted that "the hacker's actions suggest malicious intent", "the credit card information has not been recovered" and "It is possible that the potentially affected customers include youths or seniors." Despite these factors, the Organization reported that "the potential for harm is low because the credit card brands will not require that cardholders pay fraudulent charges." In my view, the likelihood of harm resulting from this incident is increased because the incident was the result of malicious intent (deliberate unauthorized intrusion), the information was potentially exposed for over 7 months, the Organization has received reports of credit card fraud, and the information has not been recovered. 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.

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 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 incident was the result of malicious intent (deliberate unauthorized intrusion), the information was potentially exposed for over 7 months, the Organization has received reports of credit card fraud, and the information has not been recovered. 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.

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 July 10, 2015. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner