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)	P2019-ND-139 (File #012928)
Date notice received by OIPC	April 4, 2019
Date Organization last provided information	April 4, 2019
Date of decision	August 15, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
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 the following information: • name, • address, • payment card number, expiry date, and 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 in Alberta via the Organization's ecommerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On March 4, 2019, the Organization learned that an unauthorized person may have acquired, through the use of malicious code, the payment card information that users entered into the e-commerce vendor's payment page. • It is believed the code was present on the website from October 29, 2018 through March 04, 2019.

	• The incident was discovered on March 4, 2019, upon a review of payment card handling practices.
Affected individuals	The incident affected 27,488 individuals.
Steps taken to reduce risk of harm to individuals	• Removed the malicious code and secured the website. • Contacted law enforcement and payment card companies. • Offered potentially affected Alberta residents identity theft protection and working with potentially impacted individuals. • Engaged a third-party expert to conduct a thorough review of our security protocols.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on April 5, 2019.
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 "…found no information indicating that Alberta customers' payment card information was actually misused, but [the Organization] could not eliminate that possibility. A potential risk is that Alberta customers' payment card information is misused, for example, by using the information to make an unauthorized purchase, and that a customer might be held responsible for that purchase." In my view, a reasonable person would consider the contact 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 reported "We think the risk is very low. Even if there were unauthorized purchases, the relevant payment card companies … have committed to protect card users against financial loss for unauthorized transactions." In my view, a reasonable person would consider the likelihood of harm resulting in this case is increased because the incident appears to be the result of deliberate, malicious action. The information was exposed for approximately 4 months. 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.	

A reasonable person would consider the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting in this case is increased because the incident appears to be the result of deliberate, malicious action. The information was exposed for approximately 4 months. 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 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 by letter on April 5, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner