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	Pentair Aquatic Eco Systems, Inc. (Organization)
Decision number (file number)	P2018-ND-025 (File #007580)
Date notice received by OIPC	January 26, 2018
Date Organization last provided information	January 26, 2018
Date of decision	February 5, 2018
Summary of decision	There is a real risk of significant harm to the individual in Alberta affected by this incident. The Organization is required to notify the individual 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 all or some of the following information: • name, • address, • telephone number, • email address, and • payment card number, expiry date and security code (CVV). This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's ecommerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 2, 2018, the Organization identified unauthorized computer code added to the checkout page of its online store at https://pentairaes.com.

	• The Organization investigated and found that the code may have been present and capable of capturing information entered during the checkout process from December 19, 2017 to January 2, 2018. • The incident was discovered on January 2, 2018 during a routine scan.
Affected individuals	The incident affected 1 resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Strengthening the security of the ecommerce platform and working with vendors and security experts to enhance security. • Established dedicated call centre to answer questions about the incident.
Steps taken to notify individuals of the incident	The Organization reported that it is mailing notification letters to the potentially affected individuals as of January 26, 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 the "potentially affected payment card numbers could be used to make fraudulent charges elsewhere online; however, payment card network rules generally state that cardholders are not responsible for fraudulent charges that are timely reported." In my view, the financial information at issue could be used to cause the harms of identity theft and fraud. In addition, email address could be used to cause the harm of phishing. 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 that "Because the payment card network rules state that cardholders are not responsible for fraudulent charges that are timely reported, there is no risk of significant harm to the potentially affected Alberta residents. To further diminish the likelihood of harm, [the Organization] is specifically recommending that potentially affected individuals remain vigilant to the possibility of fraud by reviewing their account statements and credit reports for unauthorized activity." 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 (deliberate intrusion and installation of malware). Further, the information may have been exposed for two weeks.

	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 individual in Alberta.

The financial information at issue could be used to cause the harms of identity theft and fraud. In addition, email address could be used to cause the harm of phishing. These are significant harms. 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 (deliberate intrusion and installation of malware). Further, the information may have been exposed for two weeks. 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 individual in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

The Organization reported that it is mailing notification letters to the potentially affected individuals as of January 26, 2018. The Organization is not required to notify the affected individual in Alberta again.

Jill Clayton
Information and Privacy Commissioner