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	Zero Technologies, LLC d/b/a Zero Water (Organization)
Decision number (file number)	P2019-ND-178 (File #013600)
Date notice received by OIPC	July 22, 2019
Date Organization last provided information	July 22, 2019
Date of decision	November 27, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individuals whose personal 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 is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	Information involved in the breach may have included: • name, • credit or debit card number, type, expiry date, and security code, • billing and shipping address, • telephone number, • email address, and • account password (if provided). 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.zerowater.com.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization received a report of unusual card activity from its credit card processor. • The Organization investigated, and determined that a vulnerability existed on its website that would permit access to certain customer payment card information if the vulnerability was exploited. • On or around May 24, 2019, the investigation determined that there was evidence that the vulnerability was exploited and that there was unauthorized access to payment card information.
Affected individuals	The incident affected twenty-nine Alberta residents.
Steps taken to reduce risk of harm to individuals	• Providing written notice of the incident to other state regulators as necessary. • Enhanced security measures.
Steps taken to notify individuals of the incident	Affected individuals were provided with written notice beginning on July 12, 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 did not specifically identify the potential harm(s) that might result from this incident, but said that it is "providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud". In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Credentials could be used to compromise other online accounts. 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 did not specifically assess the likelihood of harm resulting from this incident. In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach appears to be the result of malicious intent (exploited vulnerability, unauthorized access). The Organization did not report how long the information was potentially 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 that the contact and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Credentials could be used to compromise other online accounts. These are significant harms. The likelihood of harm resulting from this incident is increased as the breach appears to be the result of malicious intent (exploited vulnerability, unauthorized access). The Organization did not report how long the information was potentially 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 individuals were provided with written notice beginning on July 12, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner