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	Zumiez Canada Holdings Inc. (Organization)
Decision number (file number)	P2021-ND-209 (File #019907)
Date notice received by OIPC	March 5, 2021
Date Organization last provided information	March 5, 2021
Date of decision	November 1, 2021
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"	The incident involved some or all of the following information: • name, • shipping and billing address, • email address, • telephone number, • payment card number, expiry date, and card verification code. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information at issue was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 18, 2021, the Organization discovered suspicious activity involving its Canadian e-commerce platform (www.zumiez.ca). • The Organization identified and removed unauthorized script in the code the same day.

	• The added code was capable of obtaining information entered by customers during the checkout process and sending it out of its system. • The Organization's investigation show the code was first added on August 16, 2020 and there were several times between August 16, 2020 and January 16, 2021 when the added code was not present because of new code deployments. • The Organization identified the specific transactions involved and reinforced the security of its site.
Affected individuals	The incident affected 3,973 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Advised individuals to closely review payment card account statements and immediately report any unauthorized charges to the bank that issued the card. • Provided a telephone number for individuals to call with any questions they may have. • Implemented additional security measures. • Notified the payment cards network. • Notified law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on March 5, 2021.
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, *It is possible that unauthorized charges could be made to involved payment cards.* 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 the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all 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, *The likelihood of harm is very low. [The Organization] advised individuals to closely review payment card account statements and immediately report any unauthorized charges to the bank that issued the card. Payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported.* In my view, a reasonable person would consider 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). 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. Further, the information may have been exposed for approximately 4 ½ months.

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 the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all 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). 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. Further, the information may have been exposed for approximately 4 ½ months.

I require the Organization to notify the affected individuals whose information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by letter on March 5, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner