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	Minnetonka Moccasin Company, Inc. (Organization)
Decision number (file number)	P2022-ND-020 (File #022271)
Date notice received by OIPC	April 5, 2021
Date Organization last provided information	April 5, 2021
Date of decision	April 22, 2022
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual 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's head office is in Minneapolis, MN, USA. 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: • cardholder name, • card number, • expiration date, and • card verification value. This information is about an identifiable individual 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 December 29, 2020, the Organization discovered malicious code that was inserted in its e-commerce website. • The Organization reported, if working as designed, the malicious code had the capability to capture payment card information.

	• The Organization determined that payment card information might have been exposed for customers who made purchases through minnetonkamoccasin.com between November 25, 2020 and December 25, 2020.
Affected individuals	The incident affected 38,433 individuals, including one (1) Alberta resident.
Steps taken to reduce risk of harm to individuals	• Investigated and determined scope of incident. • Removed the malicious code. • Reset of all relevant user and administrative passwords. • Implemented multi-factor authentication. • Conducted a security scan and manual review of site to ensure incident has been remediated and no persistent threats remain.
Steps taken to notify individuals of the incident	The affected individual was notified by letter on April 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 the possible harm that may occur as a result of the breach is "Payment card 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. 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, *The risk of card fraud has been mitigated. The card brands have been notified of the incident and may take remedial action, including issuance of replacement payment cards. Fraudulent charges may be refunded.* 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 one (1) month.

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. 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. 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). 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 one (1) month. I require the Organization to notify the affected individual 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 the affected individual by letter on April 5, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Cara-Lynn Stelmack
Assistant Information and Privacy Commissioner