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	Native Canada Footwear Ltd. (Organization)
Decision number (file number)	P2017-ND-124 (File #006265)
Date notice received by OIPC	August 16, 2017
Date Organization last provided information	August 16, 2017
Date of decision	August 28, 2017
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident may have involved the following information: • name, • address, • email address, • telephone number, and • debit and credit card information. 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 website.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On June 23, 2017, the Organization became aware of a potential vulnerability in the security of its website.

	• An investigation determined that malware infected the Organization's website as early as April 2015. It appears to have resided in the website until the system was taken offline on June 23, 2017 and may have allowed outside parties to acquire payment-related information from customers who made credit purchases through the website.
Affected individuals	The incident potentially affected 861 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately took the system offline and retained forensics firms to conduct a full investigation. • Conducting a thorough review of electronic systems, and retained forensic and cybersecurity professionals to test electronic systems and to upgrade security efforts. • Developing a new online shopping site. • Arranged to provide identification protection services to customers who are potentially affected by this incident. • Notified law enforcement.
Steps taken to notify individuals of the incident	Notified affected individuals in writing on August 16, 2017.
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 "Fraud and Financial loss are the principal types of harm that could result when credit card information is involved in a breach of this kind." In my view, the contact and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. Email address could be used to cause the harm of phishing. 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 it "…was the victim of a targeted criminal malware attack by unknown individuals who appear to have acted with malicious intent. … However, [the Organization] does not have sufficient evidence to conclude that individual customers have suffered actual harm or financial loss as a result of the attack and cannot say with respect to any particular customer whether he or she has been affected by the incident or has suffered any harm." In my view, the likelihood of harm is increased because the incident was the result of malicious intent (deliberate intrusion and installation of malware) and the personal information was exposed for over two years.

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. The contact and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. In addition, email address could be used to cause the harm of phishing. These are all significant harms. The likelihood of harm is increased because the incident was the result of malicious intent (deliberate intrusion and installation of malware) and the personal information was exposed for over two years. I require the Organization to notify the affected individuals in Alberta accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals in writing on August 16, 2017. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner