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	Manduka, LLC (Organization)
Decision number (file number)	P2018-ND-44 (File #008165)
Date notice received by OIPC	March 28, 2018
Date Organization last provided information	March 28, 2018
Date of decision	April 9, 2018
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 sells yoga products and accessories to consumers. Its principle address is in California. It qualifies as 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, and • payment card information (including card number, expiry date, and security code). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's ecommerce website, www.manduka.com.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On February 25, 2018, the Organization learned of a potential data security incident involving the unauthorized installation of malware on its ecommerce web platform.

	• The incident potentially exposed information provided by customers who made online purchases between February 22, 2017 and March 5, 2018.
Affected individuals	The incident may have affected 754 Canadian residents, including 109 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Immediately took steps to secure payment card information and contacted the appropriate law enforcement agencies. • Working with a forensics firm to remove malicious code and block traffic to and from malicious domains. • Secured the ecommerce platform, reduced administrative access to its ecommerce platform, changed all user and administrative passwords. • Provided affected individuals with information and resources on how they can protect themselves. • Reported the incident to payment card brands to coordinate and monitor for fraudulent activity.
Steps taken to notify individuals of the incident	All Canadian residents whose information may have been affected were notified by letter on March 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 that it provided affected individuals with "information and resources on how they can protect themselves from or address issues of fraud or identify theft." In my view, the financial information at issue could be used to cause the significant harms of fraud and identity theft.
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 "Given that [the Organization's] systems were affected by malware, and the involvement of payment information, [the Organization] is of the view that the test for mandatory breach reporting under the *Personal Information Protection Act* (Alberta) is met and that individual notification is also required (as well as being the right thing to do)." In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to malicious action (unauthorized intrusion and installation of malware). The information may have been exposed for over one year.

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 financial information at issue could be used to cause the significant harms of fraud and identity theft. The personal information was compromised due to malicious action (unauthorized intrusion and installation of malware) and may have been exposed for over one year. I require the Organization to notify the affected individuals 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 26, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner