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	Mountain Equipment Coop (Organization)
Decision number (file number)	P2019-ND-208 (File #013668)
Date notice received by OIPC	August 15, 2019
Date Organization last provided information	August 15, 2019
Date of decision	December 20, 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"	The incident involved the following information: • partial credit card details (last four digits, full name on credit card and expiry date), • gift card number (for those members who had this information on their accounts). 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 mec.ca.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization's online ecommerce platform was attacked with a botnet between the period of July 23-August 8.

	• The botnet was doing a credential stuffing attack and attempting to use stolen credentials to log into mec.ca. Some of the credentials belonged to members and so the bot was successful at logging into 2,335 member online accounts. • The breach was discovered on August 1, 2019 through log reviews by the Organization's ecommerce team.
Affected individuals	The incident affected 2,335 individuals, including 98 known residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Reset member credentials and asked members to reset their passwords. • Enhanced security of web page and starting a security review of the ecommerce application design and process with an external security consultant.
Steps taken to notify individuals of the incident	The affected individuals were notified by email on August 13, 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 reported "Based on the limited information that was exposed we do not think this will cause any harm or risk to our members." In my view, a reasonable person would consider that the attacker was able to confirm valid email addresses for certain of the Organization's customers and this information could be used for phishing purposes, increasing vulnerability to identity theft and fraud, and 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 reported there is "A very low risk of any harm or risk occurring". In my view, the likelihood of harm resulting from this incident is increased because the incident resulted from malicious action (deliberate, botnet attack) and successfully compromised member accounts over a period of 2 weeks.
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 attacker was able to confirm valid email addresses for certain of the Organization's customers and this information could be used for phishing purposes, increasing vulnerability to identity theft and fraud, and to compromise other online accounts. These are significant harms.

The likelihood of harm resulting from this incident is increased because the breach resulted from malicious action (deliberate, botnet attack) and successfully compromised member accounts over a period of 2 weeks.

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 notified by email on August 13, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner