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 Co-operative (Organization)
Decision number (file number)	P2018-ND-107 (File #008905)
Date notice received by OIPC	June 7, 2018
Date Organization last provided information	June 7, 2018
Date of decision	August 7, 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 the individuals whose 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 operates in Alberta and 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 about members: • name, • membership number, • preferred language, • address (possibly delivery address), • telephone number, • online and telephone order history, and • limited credit card information: the last 4 digits and expiry date of any credit card associated with the member's account (not full credit card number or CVV number). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On or about April 11 and 12, 2018, the Organization detected a significant number of attempted log-ins to its website, www.mec.ca, originating from a botnet. • The botnet attempted to log into the website using numerous email addresses and passwords, which were not obtained from the Organization. More than 99% of the log-in attempts were unsuccessful because the email addresses were not known to the Organization. • The Organization is unable to confirm precisely how many of its members had their online accounts accessed by the botnet; however, it believes that 27 Alberta members may have had their online accounts accessed. Of these, only 3 members had credit card information (last four digits only) stored on their account profile. • The incident was discovered April 11, 2018 by the Organization's web administrators, who noticed an unexpected increase in traffic and subsequently identified the botnet activity.
Affected individuals	The Organization notified 245 members across Canada, including 27 members with addresses in Alberta.
Steps taken to reduce risk of harm to individuals	• Reset passwords for all accounts that were successfully logged into by the botnet. • Notified affected members and advised they would be required to change their password the next time they logged into the website. • Encouraged members to change their passwords anywhere else that they have used the same credentials. • Provided affected individuals with a website to inform members as to how their personal information was compromised.
Steps taken to notify individuals of the incident	Affected individuals were sent written notifications by email on May 5, 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 "Harm would be limited to that which may result from obtaining a member's address and telephone number, and the last four digits and expiry date of the member's credit card (if the member had any credit card information associated with their account). It is unlikely that harm such as identify theft or financial loss could result from obtaining only this information. However, if this information was combined with other information available to the source of the botnet, potential harm could possibly arise from use of the combined information."

	The Organization also noted that "… successful login by the botnet would indicate that the password provided by the botnet was a viable password for the [Organization's] accounts and thus could be a viable password for other … accounts held by the member." That is, "…if an Alberta … member used the same password for other … accounts which contained more sensitive personal information, there is a potential for significant harm arising through access to such other … accounts. This is why [the Organization's] notice to potentially affected members urged such members to change their password for any account where the same password had been used." I agree with the Organization's assessment. It is unlikely that the financial information (partial credit card number) and contact information (address, telephone number) could be used to cause significant harms such as identity theft or fraud. However, compromised credentials (confirmed valid passwords), particularly if combined with other information about the member, could be used to compromise other online accounts. This is a significant harm.
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 noted a number of factors in assessing the likelihood of harm resulting from this incident, including: • "Most of the botnet log-in attempts were unsuccessful." • "The personal information in the … accounts affected was not highly sensitive." • "The personal information was exposed for a short period of time (the exposure began on April 11th and ended in the early hours of April 12th)." • "In the few instances where the botnet was successful in accessing an account, the limited personal information that was available in the account is unlikely to be sufficient to be used for criminal purposes." • "Of the 27 Alberta member accounts potentially affected, only three had any credit card information (last four digits only) stored in the account." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the incident was the result of deliberate malicious action (botnet attack) and compromised credentials (passwords), which, particularly if combined with other information about the member, could be used to compromise other online accounts.

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. I agree with the Organization's assessment that it is unlikely that the financial information (partial credit card number) and contact information (address, telephone number) could be used to cause significant harms such as identity theft or fraud. However, the incident was the result of deliberate malicious action (botnet attack) and compromised credentials (confirmed valid passwords), which, particularly if combined with other information about the member, could be used to compromise other online accounts, which is a significant harm. 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 that affected individuals were sent written notifications by email on May 5, 2018. The Organization is not required to notify the affected individuals in Alberta again.

Jill Clayton
Information and Privacy Commissioner