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	Canadian Tire Corporation Limited (Organization)
Decision number (file number)	P2017-ND-165 (File #004736)
Date notice received by OIPC	January 13, 2017
Date Organization last provided information	August 30, 2017
Date of decision	December 11, 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 the affected 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 following information was involved in this incident: • name, • address, • telephone number, • gender, • loyalty account number, • year of birth or full date of birth, • basic transactional information relating to impacted loyalty accounts ("date, dollar amount, order number and order status of the purchase(s), a description of the item(s) with SKU number(s), the store pick up location, billing address, who is picking the order up and expiry date on the credit card"). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On January 5, 2017, routine monitoring of the Organization's security system identified unusual log-in activity on the website Canadiantire.ca. The data breach was discovered on January 7, 2017 as logs were reviewed to determine whether the attack had resulted in any inappropriate access. • The Organization's investigation indicated that an unknown third party obtained customers' login information (email address and password) for a number of loyalty member accounts from an external source which is believed to be linked to previous privacy breaches in other organizations unrelated to the Organization. There was no breach of the Organization's safeguards. • The Organization took action to suspend the affected accounts. • The Organization's investigation initially found that the cyberattack occurred on January 5 and 6, 2017. However, ongoing monitoring found that attacks of a similar nature occurred at intervals between January 3 and February 6, 2017 as well as on February 14, 21, 27 and 28.
Affected individuals	A total of 100,407 individuals were affected, of which 16,248 are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Detected the increased login traffic and took action to contain the activity by blocking access to the accounts. Automated blocking rules were implemented. • Disabled sign-in and profile changes to the web and mobile sites until additional controls were implemented. • Enhanced authentication process on the web and mobile sites. • Enhanced logging, monitoring and alerting controls on the web and mobile sites. • Reset passwords. • Shared relevant threat information with peer organizations to help thwart the broader threat campaign believed to be occurring. • Posted an updated message for customers on the login page indicating best practices for setting passwords. • Reported incident to the Canadian Cyber Incident Response Centre and law enforcement. • Suspended loyalty accounts and issued new loyalty cards and account numbers.
Steps taken to notify individuals of the incident	Customers were notified beginning on January 11, 2017, between February 10 - 18, 2017 and during the week of April 17, 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 that given "the information that may have been accessed, phishing and identity theft are potential harms." The Organization also said that "Potential financial harm in respect of the loyalty accounts would be remote and insignificant" for a number of reasons, including because "Any future financial loss on the affected loyalty accounts would be mitigated by the issuance of new loyalty cards and numbers...". I agree with the Organization that the contact, identity and profile (transactional history) information at issue could be used to cause identity theft and fraud. In combination with email addresses and account credentials, this information could be used for phishing purposes, or to compromise other online accounts with the same password. 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 stated that their "investigation concluded that an unknown third party obtained login information from an external source which is believed to be linked to previous privacy breaches in other organizations unrelated to CTC. As a result, this third party may potentially continue to use it along with the additional information accessed during this incident for malicious intent." In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion) and the attackers persisted over the course of almost two months.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances, I have decided that there is a real risk of significant harm to the affected individuals as a result of this incident. The contact, identity and profile (transactional history) information at issue could be used to cause identity theft and fraud. In combination with email addresses and account credentials, this information could be used for phishing purposes, or to compromise other online accounts with the same password. These are all significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion) and the attackers persisted over the course of almost two months.

I require the Organization to notify affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation.* I understand the Organization notified affected individuals by telephone beginning on January 11, 2017 and by email in February and April 2017, in accordance with the Regulation. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner