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 (Organization)
Decision number (file number)	P2019-ND-166 (File #013325)
Date notice received by OIPC	June 3, 2019
Date Organization last provided information	June 3, 2019
Date of decision	November 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 those 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 all or some of the following information: • name, • mailing address, • email address, • telephone number(s), • date of birth, • client/loyalty ID, and • gender. 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	• The Organization reported that a threat actor used credentials compromised in previous breaches from unrelated third party companies to gain access to accounts of users who use the same credentials with the Organization.

	• The breach occurred between May 17 - 27, 2019, and was discovered on May 17, 2019 when IT Security identified unusual activity occurring on the Organization's authentication API.
Affected individuals	The incident affected 6,500 individuals, including 700 in Alberta.
Steps taken to reduce risk of harm to individuals	• Forced password reset for all impacted accounts and previous login sessions have been discontinued. • Provided all impacted individuals with instructions for resetting passwords and the importance of maintaining strong unique passwords with each entity with whom they share information. • Reported that "Cybersecurity has successfully contained the attacks through the release of an updated app with upgraded security features. Additionally effort is underway to further understand the nature of the attacks in order to reduce the **risk** of similar events."
Steps taken to notify individuals of the incident	Affected individuals were notified by letter and email on May 26-28, 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 that possible harms that might result from the incident include "Potential financial loss" and "Potential identity theft". In my view, a reasonable person would consider the contact and identity (e.g. date of birth) information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.
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 "As no banking or other financial information formed part of the information accessed, the likelihood of financial loss stemming from this incident is low". Further, "As the threat actor used credentials that were compromised in previous security breaches (at unrelated companies), the collected information gathered from multiple sources could increase the potential for phishing and identity theft, though no highly sensitive information was compromised in this breach (no government identification numbers were accessed)." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate action using compromised credentials).

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 the contact and identity (e.g. date of birth) information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate action using compromised credentials). 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 letter and email on May 26-28, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner