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)** | P2022-ND-059 (File #027607) |
| **Date notice received by OIPC** | October 3, 2022 |
| **Date Organization last provided information** | October 7, 2022 |
| **Date of decision** | October 11, 2022 |
| **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:<br>• name,<br>• mailing address,<br>• email address,<br>• phone number(s),<br>• date of birth,<br>• client/loyalty ID, and<br>• gender.<br><br>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 August 11, 2022, 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 and utilized a |

| | |
|---|---|
| | configuration error on an application programming interface (API) to circumvent security safeguards.<br>• The breach was discovered by the Organization on September 11, 2022.<br>• The breach affected certain Triangle Reward accounts and certain Canadian Tire accounts. |
| **Affected individuals** | The incident affected 8100 individuals including 1100 Alberta customers. |
| **Steps taken to reduce risk of harm to individuals** | • Took immediate steps to block attempts measures.<br>• Forced password reset on all impacted accounts.<br>• Provided instructions to affected individuals regarding resetting their passwords and the importance of maintaining strong unique passwords with each entity with whom they share information.<br>• Updated the errant site configuration of the API.<br>• Implementing controls to mitigate the risk of a similar event. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified of the incident by email on September 23, 2022 and September 26, 2022. |
| **REAL RISK OF SIGNIFICANT HARM ANALYSIS** | |
| **Harm**<br>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 the possible harms that may occur as a result of the breach are *"Potential financial loss (and) Potential identity theft."*<br><br>In my view, a reasonable person would consider the contact and identity information combined with email address, could be used for phishing or impersonation, increasing vulnerability to identity theft and fraud. Confirmed valid credentials could be used to compromise online accounts. These are significant harms. |
| **Real Risk**<br>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,<br><br>*Financial Loss:*<br>*As no banking or other financial information formed part of the information accessed, the likelihood of financial loss stemming from this incident is low.*<br><br>*Identity Theft:*<br>*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 incident appears to be the result of malicious action (deliberate intrusion). It appears the information may have been exposed for approximately one month before the Organization became aware of the breach. |

**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 contact and identity information combined with email address, could be used for phishing or impersonation, increasing vulnerability to identity theft and fraud. Confirmed valid credentials could be used to compromise online accounts. These are significant harms.

The likelihood of harm resulting from this incident is increased because the incident appears to be the result of malicious action (deliberate intrusion). It appears the information may have been exposed for approximately one month before the Organization became aware of the breach.

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 the Organization notified affected individuals by email on September 23, 2022, and September 26, 2022, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance