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) This decision concerns a report submitted by the Organization as an update to a matter that is the subject of a breach decision previously issued by the Office of the Information and Privacy Commissioner (Breach Decision P2017-ND-165).
Decision number (file number)	P2018-ND-027 (File #007394)
Date notice received by OIPC	December 13, 2017
Date Organization last provided information	December 13, 2017
Date of decision	February 5, 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 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	• The Organization previously reported that, in January 2017, routine monitoring of the Organization's security system identified unusual log-in activity on the website Canadiantire.ca. • 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. • 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. • The Organization is now reporting that, due to enhanced monitoring and detection capabilities, it has detected suspicious log-in activity that "is an evolution of the form of cyber attack used earlier this year" and "between September 19 and November 21, this account access activity increased somewhat in volume." Further, "In the more recent subsequent incidents identified, new VPNs not previously identified with suspicious activity were employed to effect the account access."
Affected individuals	There are a total of 338 affected individuals, including 33 individuals from Alberta.
Steps taken to reduce risk of harm to individuals	• Educating affected individuals about the steps they should take to change their credentials and keeping their accounts locked until these steps have been taken. • Reinstating loyalty balances that were depleted by suspect activity. • The Organization's IT Security and Enterprise Corporate Security are updating the RCMP in connection with prior briefings provided regarding the incidents.
Steps taken to notify individuals of the incident	The Organization reported that "…all potentially affected individuals are being notified by email".

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 originally 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 agreed 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. This continues to be the case for the individuals potentially affected by the recent incidents.
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 originally reported 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." I previously found that the likelihood of harm resulting from this incident was increased as the breach was the result of malicious intent (deliberate intrusion) and the attackers persisted over the course of almost two months. The Organization is now reporting the attacks have persisted from September 19 through November 21.

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 individuals potentially affected as a result of this incident.

I previously found 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 and this continues to be the case for the individuals potentially affected by the recent incidents.

I previously found that the likelihood of harm was increased as the breach was the result of malicious intent (deliberate intrusion) and the attackers persisted over the course of almost two months. The Organization is now reporting the attacks have persisted from September 19 through November 21.

I require the Organization to notify the individuals in Alberta who are potentially affected, in accordance with section 19.1 of the *Personal Information Protection Act Regulation.* The Organization has reported that "…all potentially affected individuals are being notified by email". **I require the Organization to confirm to my office within 10 days of the date of this decision that the potentially affected residents of Alberta have been notified.**

Jill Clayton
Information and Privacy Commissioner