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	Fountain Tire Ltd. (Organization)
Decision number (file number)	P2018-ND-106 (File #008654)
Date notice received by OIPC	May 11, 2018
Date Organization last provided information	May 11, 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 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The first incident involved the following information of 36 associates of the Organization: • name, • address, • date of birth, • social insurance number, • health care number, and • employee number. The second incident involved the following information of 337 associates of the Organization: • name, • address, • social insurance number, • driver's license number, • employee number, and • bank information.

	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 two separate occasions, associates with the Organization clicked on phishing emails and entered their credentials, enabling an unknown individual(s) to gain access to their email accounts. • The incidents took place on April 5, 2018 (discovered the same day) and April 16, 2018 (discovered the next day). • The Organization's investigation revealed that both compromised email accounts contained personally identifiable information of certain associates of the Organization. • The Organization has no evidence that the unauthorized individual actually accessed the personal information, but reported the information was accessible to the intruder(s). • The incidents were discovered when the associates started to receive emails from their contacts who were questioning emails sent from the associates' account.
Affected individuals	The incidents affected 337 individuals.
Steps taken to reduce risk of harm to individuals	• Immediately changed the affected login credentials. • Notified all associates on what to look for and how to avoid phishing attacks, as well as best practices around not having sensitive information saved in email accounts. • Implemented process changes for Payroll Team and Safety Team to ensure sensitive information is not saved on email accounts. • Will offer affected individuals credit monitoring services at the Organization's expense. • Planned education sessions on how to avoid these attacks. • Piloting technological controls to prevent further incidents.
Steps taken to notify individuals of the incident	The Organization reported that notification letters would be sent to affected individuals on or before May 16, 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	The Organization reported "While we have no evidence that the unauthorized individual or individuals actually accessed or acquired the associates' information, the nature of the information involved could lead to financial loss, fraud, identity theft and negative effects on a credit record." I agree with the Organization's assessment. The identity, contact and

non-trivial consequences or effects.	financial information at issue could be used to cause the significant harms of identity theft and fraud, financial loss and negative effects on a credit record.
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 "We believe the likelihood that harm could result is relatively low. While we know the attacker(s) connected to the associate's email via outlook, we do not have any evidence that they saved a copy of the email contents offline. It is most likely they were looking to acquire the login credentials for continued attacks into the [Organization's] network and/or third parties through email contacts. However we cannot rule out the possibility that the attacker(s) saved a copy of the email contents offline so we are erring on the side of caution in reporting the incident and notifying all individuals whose information was available on the email contents." In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to malicious phishing emails on two separate occasions. The intruder had access to the email accounts at issue, and the Organization cannot confirm the personal information was not copied, forwarded or used by the unauthorized individual.

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 identity, contact and financial information at issue could be used to cause the significant harms of identity theft and fraud, financial loss and negative effects on a credit record. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to malicious phishing emails on two separate occasions. The intruder had access to the email accounts at issue, and the Organization cannot confirm the personal information was not copied, forwarded or used by the unauthorized individual.

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 the Organization reported that notification letters would be sent to affected individuals on or before May 16, 2018. **I require the Organization confirm to my office in writing within 10 days of the date of this decision that this has been done.**

Jill Clayton
Information and Privacy Commissioner