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	Loblaw Companies Limited (Organization)
Decision number (file number)	P2019-ND-032 (File #006114)
Date notice received by OIPC	July 24, 2017
Date Organization last provided information	July 24, 2017
Date of decision	February 19, 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, • address, • telephone number, • email address, and • order history. If loyalty cards were linked to the affected accounts, then the following information may also have been at issue: • PC Plus points and personalized offers (Click & Collect websites); • Optimum points balance (beautyboutique.ca); and • PC Plus points balance (JoeFresh.com and JoeFresh.ca) This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's websites.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• Between May 12, 2017 and July 7, 2017, automated "credential stuffing" attacks occurred against web properties owned by the Organization. • High traffic volumes led the Organization to investigate what appeared to be unauthorized access to user accounts and logins that were likely unauthorized. • On June 13, 2017, the Organization received telephone calls from users reporting they received an automated message from one of the Organization's online sites indicating their user profile had changed. The users had not changed their profile. • The Organization immediately deactivated affected user accounts and loyalty cards. • The Organization believes that stolen credentials (email addresses and passwords) from other mass breaches were used to access accounts on the Organization's web properties.
Affected individuals	The total number of affected individuals is 28,958. The Organization said it was not possible to identify all users by jurisdiction. Based on the information available, there were 5,289 Alberta residents affected by the breach.
Steps taken to reduce risk of harm to individuals	• Implemented rate limiting on IP addresses accessing web properties and API. • Implemented a captcha-like system designed to establish that a computer user is a human. • Deployed a cap on the number of concurrent users allowed to log in. • Forced password rest for all the affected customers. • Build automated spike detection. • Analyzing logs for malicious activity. • Monitoring any email address changes for each of the web properties to determine whether the change is legitimate or malicious. • Monitoring of logs for malicious activity and manual spike monitoring.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on June 29, 2017 and July 19, 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 identified "Identity theft" and "Risk of increased phishing attempts" as types of harm that could result from the breach, and indicated the level of harm to be "medium". I agree with the Organization's assessment. A reasonable person would consider that the contact and profile information (order history and point balance) 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 "The type of personal information accessed, the quantity of the accounts accessed, i.e. the number that show unique and unauthorized log in and the nature of the activity (fraud), is such that [the Organization] believes that the risk of harm may be enough to reach the threshold where there is a real risk of significant harm to the affected individuals." 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 intrusion). Further, the information may have been exposed for approximately 45 days.

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 that the contact and profile information (order history and point balance) 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 intrusion). Further, the information may have been exposed for approximately 45 days.

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 June 29, 2017 and July 7, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner