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 Ltd. (Organization)
Decision number (file number)	P2019-ND-149 (File #008002)
Date notice received by OIPC	March 26, 2018
Date Organization last provided information	October 26, 2018
Date of decision	August 20, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
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, • points balance, • email address, and • order history. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization launched a new loyalty program on February 1, 2018. • After the launch, the Organization identified suspicious spikes in traffic. The first attack noted was on February 14, 2018, followed by attacks on other ecommerce websites in March 2018 (PC Optimum, Joe Fresh and Digital Pharmacy). • The Organization investigated, and determined the PC Optimum website was targeted by automated bots in an attempt to authenticate members' login credentials (i.e. email address and password) and then use these credentials to access member accounts. • With respect to Digital Pharmacy, the threat actor(s) were not able to access any personal information in patients' online accounts. Nonetheless, the Organization determined that the threat actor(s) were likely using the ecommerce and Digital Pharmacy sites to authenticate credentials in order to access member accounts and steal points. • The Organization "believes that stolen login credentials (i.e. email addresses and passwords) from previous mass security breaches (e.g. Yahoo and LinkedIn) were used by threat actors in attempts to access the large number of recently created PC Optimum accounts".
Affected individuals	The incident affected 45,078 individuals of which 4,061 were residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately investigated the incident. • Enhanced technological protections and monitoring capabilities to identify and block bot attacks. • Contained the incident. • Implemented a forced password reset on potentially impacted accounts. • Advised impacted individuals. • Instructed individuals to create a new and strong password during their next login (letters, numbers, and characters). • Temporarily reset rate limit on the click and collect application to prevent any inbound traffic to the application prior to full deployment of enhances protections. • Notified private sector privacy commissioner.
Steps taken to notify individuals of the incident	Affected individuals were notified in writing on March 12, 2018 and March 26, 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 non-trivial consequences or effects.	The Organization reported that it informed affected individuals "…that the information which may have been displayed could put them at increased risk of phishing attempts." I agree with the Organization's assessment. A reasonable person would consider that email address, particularly when combined with other contact information and order history, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. To the extent the threat actors were able to authenticate credentials, other online accounts may also be at risk of compromise.
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 "…while the type of information that may have been accessed by the threat actor(s) was not sensitive in nature … given the quantity of the accounts accessed (i.e. the number that show unauthorized access), and the nature of the activity (fraud), [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." Further, the Organization said "Where customers have identified that their points have been stolen, [the Organization] will be redeeming their points in full to limit any financial harm to its members resulting from the incident." I agree with the Organization's assessment. A reasonable person would consider 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), and a significant number of accounts were accessed for fraudulent purposes.

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 email address, particularly when combined with other contact information and order history, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. To the extent the threat actors were able to authenticate credentials, other online accounts may also be at risk of compromise. 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), and a significant number of accounts were accessed for fraudulent purposes.

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 in writing on March 12, 2018 and March 26, 2018, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner