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	Sobeys Capital Incorporated (Organization)
Decision number (file number)	P2023-ND-006 (File #027997)
Date notice received by OIPC	November 8, 2022
Date Organization last provided information	January 25, 2023
Date of decision	February 2, 2023
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 headquartered in Mississauga, Ontario, and 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: **For individuals affected in a credential stuffing attack, and "unauthorized API[1] calls … to a … customer data cloud":** • name, • date of birth, • telephone number, • email address, • postal address, • username, • password, • last four digits of credit card number, • credit card expiry date, • knowledge that username/password combinations were valid, • rewards program numbers (Voila, Scene, Air Miles), and • social media name and URL to social media page.

[1] Application Programming Interface.

	For individuals affected in an attack against the Organization's "digital experience API": • name, • Scene+ number, • Scene account status, • Scene point balance, • digital barcode (as a string), and • date individual became a member. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On or about October 31, 2022, the Organization became aware that various online services were targets of unauthorized access. • An investigation found multiple occurrences between October 29 and December 22, 2022, where one or more threat actor(s) attempted to - or successfully - accessed personal information via unauthorized API calls and a credential stuffing attack. • With respect to the credential stuffing attack, the Organization believes threat actor(s) obtained and used compromised credentials from "a third-party website breach, phishing attack or password dump."
Affected individuals	The incident affected "approximately 4,995 individuals residing in Alberta."
Steps taken to reduce risk of harm to individuals	• Investigated the incident. • Blocked suspicious IP addresses. • Disabled affected user accounts and forced password resets. • Enhanced certain technical safeguards. • Implementing enhanced authentication requirements, including multifactor authentication (MFA).
Steps taken to notify individuals of the incident	The Organization reported on January 25, 2023: *[A]ffected individuals have received informal notification in connection with this incident*. *[The Organization] has, or has directed its loyalty partner to do so on its behalf where appropriate, contacted all affected users, as applicable, to notify them that they are locked out of their account and must reactivate their accounts with a*

	password reset and/or to notify them that their Scene+ numbers were frozen and have received a new number. *Logistics for formal individual notification (as prescribed by PIPA) to potentially affected individuals is currently being coordinated. Notification is expected to commence in approximately 2 to 3 weeks*.
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 on January 25, 2023: *There is a possibility that that the [sic] name and email address could be used to conduct phishing attempts.* *Additionally, there is a possibility that the Scene+ numbers and related information may be used for fraudulent redemption of Scene+ points.* In my view, a reasonable person would consider that the identity (name, date of birth), contact (email, telephone number, postal address), credentials, partial credit card number, credit card expiry date, social media, and rewards / loyalty program information could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing affected individuals' vulnerability to identity theft and fraud. Knowledge that credential combinations were valid could be used to compromise other online accounts. These are significant harms.
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 on November 8, 2022: *… there is a low likelihood that harm will result from this incident, given the lack of evidence of any actual access to, exfiltration of or misuse of customer personal information…* On January 25, 2023, the Organization reported the "possibility" of harm(s) as set out in the harms analysis above. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because personal information was compromised due to the malicious action of one or more threat actors (credential stuffing attack, unauthorized API calls). A lack of evidence of misuse does not mitigate against future harm as phishing, identity theft, and fraud can occur months or years after a breach. Further, the Organization became aware of the incident(s) as early as October 31, 2022 and, as of the date of this decision, had not formally notified affected individuals. Affected individuals may not have taken steps to mitigate risk of harm.

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 (name, date of birth), contact (email, telephone number, postal address), credentials, partial credit card number, credit card expiry date, social media, and rewards / loyalty program information could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing affected individuals' vulnerability to identity theft and fraud. Knowledge that credential combinations were valid could be used to compromise other online accounts. These are significant harms. The likelihood of harm resulting from this incident is increased because personal information was compromised due to the malicious action of one or more threat actors (credential stuffing attack, unauthorized API calls). A lack of evidence of misuse does not mitigate against future harm as phishing, identity theft, and fraud can occur months or years after a breach. **The Organization is required to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and is required to confirm to my Office, within ten (10) days of the date of this decision, that affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.** If the Organization is unable to notify affected individuals under section 19.1(1), it may consider making a submission to my office pursuant to section 19.1(2) of the Regulation within seven (7) days of this decision. The submission must include reasons why direct notification is unreasonable in the circumstances and include a plan on how it intends to notify affected individuals indirectly.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance