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-007 (File #028700) |
| **Date notice received by OIPC** | November 15, 2022 |
| **Date Organization last provided information** | January 24, 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:<br>• name,<br>• email address,<br>• residential address,<br>• full or partial:<br>  ○ Social Insurance Number,<br>  ○ "other governmental identification",<br>  ○ bank account number,<br>• employment information, including:<br>  ○ salary information,<br>  ○ union rank,<br>  ○ leave of absence information,<br>  ○ workplace accident reports, and<br>  ○ performance review data.<br><br>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 November 3, 2022, the Organization "became aware of a potential IT issue."<br>• On November 4, 2022, the Organization determined it was victim to a ransomware attack when "multiple … systems were encrypted by an unauthorized third party."<br>• An investigation "determined that an unauthorized third party was first able to access [the Organization's] network on October 14, 2022 when [an] employee downloaded and executed a file sent to the individual in connection with a phishing attempt." |
| **Affected individuals** | The incident affected "approximately 115,175 … employees in the Province of Alberta." |
| **Steps taken to reduce risk of harm to individuals** | • Launched an investigation with the assistance of external cybersecurity expertise.<br>• Notified law enforcement and the Canadian Centre for Cybersecurity.<br>• Offering credit and identity monitoring services to certain affected individuals.<br>• Enhanced certain technical and administrative safeguards.<br>• Conducting additional assessments to identify and remediate vulnerabilities. |
| **Steps taken to notify individuals of the incident** | In its January 24, 2023 update, the Organization reported:<br><br>*Logistics for the notification to potentially affected individuals is currently being coordinated. Notification is expected to commence within approximately the next two to three weeks [by] postal mail and email (when no postal address is available)* |
| **REAL RISK OF SIGNIFICANT HARM ANALYSIS** | |
| **Harm**<br>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. | On January 24, 2023, the Organization reported:<br><br>*[G]iven that the potentially affected personal information includes email addresses, there may be an increased risk of phishing to potentially affected individuals. Additionally, potentially affected individuals whose sensitive personal information may have been impacted … may be at an increased risk of identity theft or fraud.*<br><br>I accept the Organization's assessment. A reasonable person would consider that the identity (name, Social Insurance Number, other |

| | |
|---|---|
| | government identification), contact (email, residential address), and employment (salary, union rank, leave of absence information, accident reports, performance review data) information could be used to cause the harms of identity theft, fraud, and possibly embarrassment, hurt or humiliation. Email addresses could be used for the purposes of phishing, increasing affected individuals' vulnerability to the above. These are significant harms. |
| **Real Risk**<br>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. | On January 24, 2023, the Organization reported:<br><br>*To date [the Organization's] forensic investigation has found no evidence of actual access to or exfiltration of personal information from the impacted … systems. However, [The Organization] cannot rule out the possibility of access to or exfiltration of certain personal information contained on the impacted servers.*<br><br>*To date, [the Organization] is not aware of any actual harm to potentially affected individuals. [The Organization] also has no indication that any personal information potentially affected in this incident has been publicly posted, including based on dark web monitoring conducted in the wake of the incident.*<br><br>*Given the nature of the incident and the lack of any actual harm to date to potentially affected individuals, Sobeys maintains that there is a relatively low likelihood of actual harm to potentially affected individuals.*<br><br>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 unauthorized third party (phishing / deliberate intrusion, deployment of ransomware, possible exfiltration of personal information).<br><br>A lack of evidence that personal information was misused, exfiltrated, or disclosed on the dark web, does not mitigate against future harm as identity theft, fraud, and phishing can occur months or years after a breach.<br><br>The Organization stated that even though it has not found evidence of actual access to or exfiltration of personal information, it cannot rule out the possibility of access or exfiltration of "certain personal information contained on the impacted servers." |

**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, Social Insurance Number, other government identification), contact (email, residential address), and employment (salary, union rank, leave of absence information, accident reports, performance review data) information could be used to cause the harms of identity theft, fraud, and possibly embarrassment, hurt or humiliation. Email addresses could be used for the purposes of phishing, increasing affected individuals' vulnerability to the above. These are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unauthorized third party (phishing / deliberate intrusion, deployment of ransomware, possible exfiltration of personal information).

The Organization stated that even though it has not found evidence of actual access to or exfiltration of personal information, it cannot rule out the possibility of access or exfiltration of "certain personal information contained on the impacted servers."

A lack of evidence that personal information was misused, exfiltrated, or disclosed on the dark web, does not mitigate against future harm as identity theft, fraud, and phishing 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