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** | Imperial Oil Limited (Organization) |
| **Decision number (file number)** | P2018-ND-019 (File #005613) |
| **Date notice received by OIPC** | May 16, 2017 |
| **Date Organization last provided information** | December 5, 2017 |
| **Date of decision** | January 29, 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 those individuals 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:<br>• name,<br>• billing address,<br>• account password,<br>• loyalty points, and<br>• email address.<br><br>This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from Albertans via the Organization's website. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |
| **Description of incident** | • On April 10, 2017, the Organization learned that its loyalty program website, which is hosted by a vendor, was attacked by an unknown third party using IDs and passwords. |

| | |
|---|---|
| | • The attack attempted to login and access customer loyalty accounts.<br>• The attack was discovered by the Organization's vendor as part of normal alerting on website traffic.<br>• The Organization investigated and believes that usernames and passwords may have been available to the unauthorized third party through illicit means (i.e. dark web). There is no evidence that the usernames and passwords were acquired from the Organization.<br>• The attack occurred between April 9, 2017 and April 10, 2017. |
| **Affected individuals** | The incident affected 3,042 Albertans. |
| **Steps taken to reduce risk of harm to individuals** | • Immediately shut down the websites, investigated the attack and implemented corrective measures.<br>• Required individuals to re-set all of their logins and passwords.<br>• Enhanced Geo-blocking with IP location control to access the site. IP address will be blocked after increased logon attempts.<br>• Ensured that any inappropriately accessed loyalty points were completely replaced/refunded.<br>• Issued new loyalty accounts and cards. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified on April 28, 2017 by email. |
| **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. | The Organization reported that "the harm that could result are believed to be minimal, but could potentially include denial of access to loyalty accounts for a short period of time, or loss of loyalty points if fraudulently redeemed."<br><br>Additionally, the Organization reported that it "believes that the users' username and passwords used to gain access to [its loyalty] website were sources externally from the [loyalty] website…this information may have been available to those that perpetrated the access attempts through illicit means (i.e. the dark web). Operating under the assumption that users may have the same usernames and passwords for multiple websites, it is believed that the perpetrators simply used this available log-in information to attempt to access the [loyalty] website."<br><br>In my view, the information at issue, in certain cases, could be used to access accounts (albeit limited) and cause mischief (closing an account, changing an address etc.). |

| | |
|---|---|
| | As well, email addresses, particularly in combination with contact and profile information (name, password, loyalty member) could be used for phishing purposes or to compromise other online accounts with the same password. 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. | The Organization reported that it "assessed the risk of harm to be low. However, out of an abundance of caution, and in recognition of the fact that multiple pieces of low-risk personal information were gathered at the same time, [the Organization] did think it was appropriate to notify the Alberta OIPC."<br><br>In my view, 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). |

**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 information at issue, in certain cases, could be used to access accounts (albeit limited) and cause mischief (closing an account, changing an address etc.). As well, email addresses, particularly in combination with contact and profile information (name, password, loyalty member) could be used for phishing purposes or to compromise other online accounts with the same password. 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 unknown third party (deliberate intrusion).

I require the Organization to notify the affected individuals 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 April 28, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner