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** | Yahoo! Inc. (Organization) |
| **Decision number (file number)** | P2021-ND-345 (File #004190) |
| **Date notice received by OIPC** | October 25, 2016 |
| **Date Organization last provided information** | November 6, 2017 |
| **Date of decision** | March 14, 2022 |
| **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:<br>• name,<br>• email address,<br>• telephone number,<br>• date of birth,<br>• hashed password,<br>• encrypted or unencrypted security questions and answers.<br><br>This information is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |
| **Description of incident** | • On August 1, 2016, media reported a hacker's assertion that the Organization's data had been obtained. |

| | |
|---|---|
| | • The Organization investigated and found evidence that a copy of certain user account information "may have been transferred" from the company's network in November 2014.<br>• On September 22, 2016, the Organization announced that a copy of certain user account information had been stolen by what the Organization "continues to believe is a state-sponsored actor".<br>• In a later submission, the Organization reported the breach involved data that appeared to have been stolen in August 2013. |
| **Affected individuals** | The Organization reported over 14 million Canadian user accounts were affected, including approximately 74,000 accounts in Alberta, of which 9,327 were inactive. |
| **Steps taken to reduce risk of harm to individuals** | • Retained an external forensics firm to investigate.<br>• Invalidated unencrypted security questions and answers and asked affected users to change passwords.<br>• Encouraged users who had not changed their passwords since 2014 to do so.<br>• Encouraged users to change passwords/security questions and answers for other online accounts.<br>• Posted a notice on the Organization's website, issued a press release, created a dedicated FAQ page.<br>• Worked closely with law enforcement.<br>• Reported the breach to data protection authorities.<br>• Enhanced systems that detect and prevent unauthorized access to user accounts and strengthened defences against threats to user security. |
| **Steps taken to notify individuals of the incident** | The Organization reported that it provided notice to all Canadian users beginning on September 22, 2016, and confirmed all affected individuals were notified. The Organization notified additional Canadian users beginning on October 3, 2017. |
| **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 did not specifically identify the type of harm(s) that might result from this breach, but its notice to affected individuals said:<br><br>*We encourage you to follow these security recommendations:*<br><br>• *Change your password and security questions and answers for any other accounts on which you used the same or similar information used for your... account.*<br>• *Review your accounts for suspicious activity.* |

| | |
|---|---|
| | • *Be cautious of any unsolicited communications that ask for your personal information or refer you to a web page asking for personal information.*<br>• *Avoid clicking on links or downloading attachments from suspicious emails.*<br><br>In my view, a reasonable person would consider the contact and identity information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Unencrypted credentials could be used to compromise other online accounts. 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 did not provide its assessment of the likelihood of significant harm resulting from this breach.<br><br>In my view, a reasonable person would consider the likelihood of significant harm resulting is increased because the incident was the result of malicious intent (deliberate intrusion, theft by state-sponsored actor). The Organization reported the data theft occurred in August 2013, but was not confirmed until September 2016. |

**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 the contact and identity information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Unencrypted credentials could be used to compromise other online accounts. These are significant harms. The likelihood of harm resulting is increased because the incident was the result of malicious intent (deliberate intrusion, theft by state-sponsored actor). The Organization reported the data theft occurred in August 2013, but was not confirmed until September 2016.

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 all Canadian users beginning on September 22, 2016, and notified additional Canadian users beginning on October 3, 2017, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner