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** | Rooster Teeth Productions, LLC (Organization) |
| **Decision number (file number)** | P2021-ND-075 (File #014147) |
| **Date notice received by OIPC** | December 11, 2019 |
| **Date Organization last provided information** | December 11, 2019 |
| **Date of decision** | March 9, 2021 |
| **Summary of decision** | There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the 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><br>• name,<br>• email address,<br>• telephone number<br>• physical address, and<br>• payment card information, including CVV code and expiry date.<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 in Alberta via the Organization's website, therefore PIPA applies. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |

| | |
|---|---|
| **Description of incident** | • On December 2, 2019, the Organization received complaints from consumers about its checkout process.<br>• The Organization investigated and discovered that malicious code had been added to its ecommerce site (site) earlier the same day. The malicious code directed users to a spoofed webpage where they were asked to enter their payment card details in order to complete their purchases. Users who completed the payment card details page were then directed to the real webpage, where they were asked to complete the forms again.<br>• The Organization's investigation determined that a phishing email had been sent to a small distribution list, and administrator credentials were likely obtained as a result.<br>• Seven Alberta consumers were returned from the spoofed webpage to the site and completed their payment details within the correct form. It is possible that these users provided information on the spoofed webpage.<br>• Five Alberta users failed to return and complete the correct form on the site. These individuals may or may not have provided the same information on the spoofed webpage. |
| **Affected individuals** | The incident affected 12 individuals residing in Alberta |
| **Steps taken to reduce risk of harm to individuals** | • Removed the malicious code from the site.<br>• Took other steps to secure the site against further unauthorized access.<br>• Notified potentially affected individuals and included information on steps individuals can take to help protect themselves.<br>• Offered affected individuals free monitoring services for one year. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by letter on December 11, 2019 |
| **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 any harm that might result from this incident, but its notification to affected individuals stated "We encourage you to remain vigilant for incidents of fraud and identity theft by carefully reviewing your payment card or personal account statements for unauthorized charges and monitoring free credit reports for fraudulent activity or errors resulting from the incident."<br><br>In my view, a reasonable person would consider that the financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for |

| | |
|---|---|
| | phishing purposes, increasing vulnerability to identity theft and fraud. 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 specifically provide an assessment of the likelihood that significant harm would result from this incident.<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 and installation of malware). The Organization did not report how long the information may have been exposed. |

**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 the financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Credentials could be used to compromise other online accounts. 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 and installation of malware). The Organization did not report how long the information may have been exposed.

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 affected individuals in a letter dated December 11, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner