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** | FabFitFun, Inc. (Organization) |
| **Decision number (file number)** | P2021-ND-149 (File #017328) |
| **Date notice received by OIPC** | September 21, 2020 |
| **Date Organization last provided information** | May 14, 2021 |
| **Date of decision** | June 2, 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 headquartered in Los Angeles, California, in the United States. The incident affected the new member sign up pages of its website.<br><br>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 some or all of the following information:<br><br>• credit/ debit card information (name, address, account number, expiry date, and verification code),<br>• email address,<br>• customer password.<br><br>This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |

| | |
|---|---|
| **Description of incident** | • On August 7, 2020, the Organization discovered that an unauthorized third party had inserted malicious code on portions of its website that may have enabled them to capture certain information in connection with customer sign ups.<br>• The incident affected new member sign up pages of the website during the period between April 26, 2020 and May 14, 2020, and between May 22, 2020 and August 3, 2020. |
| **Affected individuals** | The incident affected 5,553 individuals, including approximately 1,974 Alberta residents. |
| **Steps taken to reduce risk of harm to individuals** | • Offered identity protection services to affected individuals.<br>• Removed malicious code and secured the website.<br>• Reset passwords for all users.<br>• Reported incident to law enforcement. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by email on September 15, 2020. |
| **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 "Because certain payment card information was accessible, it is possible that such information could be used for fraudulent transactions."<br><br>I agree with the Organization's assessment. A reasonable person would consider that the contact, credentials and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Credentials could be used to compromise other online accounts. These are all 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…<br><br>*… believes harm is unlikely because it has provided notice of this incident to affected individuals and alerted them to this issue. In addition, [the Organization] included an offer for Identity Protection Services to individuals to help protect against misuse of information.*<br><br>In my view, a reasonable person would consider 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). It appears the information was exposed for approximately 3 months. |

| 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.<br><br>A reasonable person would consider that the contact, credentials and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Credentials could be used to compromise other online accounts. These are all significant harms.<br><br>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). It appears the information was exposed for approximately 3 months.<br><br>I require the Organization to notify the affected individuals whose information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).<br><br>I understand the Organization notified affected individuals by email on September 15, 2020 in accordance with the *Regulation*. The Organization is not required to notify the affected individuals again. |

Jill Clayton
Information and Privacy Commissioner