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** | L Brands, Inc. (Organization) |
| **Decision number (file number)** | P2022-ND-046 (File #022873) |
| **Date notice received by OIPC** | August 23, 2021 |
| **Date Organization last provided information** | August 23, 2021 |
| **Date of decision** | August 31, 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 a specialty retailer based in Columbus, Ohio.<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 all or some of the following information:<br><br>• name,<br>• contact information (postal address, phone number and/or email address), and<br>• injury reports prepared by SafetyCall (adverse reactions, minor injuries suffered, body part affected, how long symptoms lasted, known allergies, whether individual consulted a medical professional and similar reactions experienced).<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** | • SafetyCall provides adverse event reporting services related to consumer products for the Organization. SafetyCall uses a sub-processor, NetGain, for data hosting services.<br>• On November 24, 2020, SafetyCall first became aware of a potential security issue, which culminated in the launch of ransomware on December 3, 2020.<br>• On December 14, 2020, SafetyCall informed the Organization that NetGain experienced a potential security incident and started investigating the incident.<br>• On January 25, 2021, NetGain informed SafetyCall that the Organization's customer data might have been taken from its network as part of the attack.<br>• On July 8, 2021, the Organization received potentially compromised records from SafetyCall and began a review to determine whether any sensitive data was located within them. |
| **Affected individuals** | The incident affected 18 individuals, whose information was collected in Alberta. |
| **Steps taken to reduce risk of harm to individuals** | <u>Service providers:</u><br>• Took its systems offline as a precautionary measure and initiated response protocols.<br>• Launched an investigation into the attack with the assistance of third party cybersecurity and forensic specialists.<br>• Implemented business continuity plans to minimize disruption to customers.<br>• Ensured the ongoing security of its systems.<br>• Notified law enforcement authorities.<br>• Worked with cybersecurity and forensic specialists to determine what may have happened and what information may have been involved.<br>• Notified affected individuals on the Organization's behalf.<br><br><u>Organization:</u><br>• Activated its security incident response plan and deployed legal, IT and other resources to monitor the investigation.<br>• Asked SafetyCall to investigate the matter as quickly as possible, prioritize the analysis of SafetyCall data pertaining to the Organization, and have regular, weekly meetings with the Organization to keep it apprised of the status and results of the investigation.<br>• Obtained the records from SafetyCall and began a comprehensive review with outside data privacy professionals to determine whether any sensitive data was located within them. |

| | |
|---|---|
| | • Provided affected individuals with precautionary measures to protect their personal information. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by letter on August 23, 2021. |
| **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 provide an assessment of the likelihood that harm will occur, but its notification to affected individuals stated:<br><br>*We have no information to date indicating that your information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.*<br>*• Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.*<br>*• Review your Explanation of Benefits (EOB) which is a statement you receive from your health insurance company after you have a medical visit. Follow up with your insurance company or care provider's billing office for any items you do not recognize. If necessary, contact the care provider on the EOB statement and ask for copies of medical records from the date of the potential access (noted above) to current date at no expense to you.*<br>*• Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.*<br><br>In my view, a reasonable person would consider the contact and medical information at issue could be used to cause the significant harms of fraud, embarrassment, hurt or humiliation. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. 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 | The Organization reported<br><br>*We have no information to date indicating that your information involved in this incident was or will be used for any unintended purposes.* |

| | |
|---|---|
| between the incident and the possible harm. | 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, ransom demand). The Organization reported, "*We have no information to date indicating that your information involved in this incident was or will be used for any unintended purposes.*" The lack of reported incidents resulting from this breach to date is not a mitigating factor. Phishing, identity theft and fraud can occur months and even years after a data breach. |

**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 contact and medical information at issue could be used to cause the significant harms of fraud, embarrassment, hurt or humiliation. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all 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, ransom demand). The lack of reported incidents resulting from this breach to date is not a mitigating factor. Phishing, identity theft and fraud can occur months and even years after a data breach.

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 by letter on August 23, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance