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** | Leafly Holdings, Inc. (Organization) |
| **Decision number (file number)** | P2020-ND-013 (File #013727) |
| **Date notice received by OIPC** | October 9, 2019 |
| **Date Organization last provided information** | October 9, 2019 |
| **Date of decision** | February 13, 2020 |
| **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 information at issue includes:<br>• email address and username associated with accounts in 2016, and the then-current password (passwords were encrypted and the key was not compromised), and<br>• "less than 15% of the records contained additional information voluntarily provided by users, consisting of name, age, gender, location, zip code and SMS number" and potentially "additional data, including user reviews".<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 September 30, 2019, the Organization was contacted by a security researcher who advised that he had obtained a set of the Organization's user records.<br>• The Organization investigated and found that the records were from a legacy database that was last updated in July 2016. This database was separate from the Organization's production database, and has since been decommissioned. |
| **Affected individuals** | The Organization reported the incident affected "…approximately 8700 records with .ca email domains, and while presumably some of these users reside in Alberta, it has no further information". |
| **Steps taken to reduce risk of harm to individuals** | • Invited users to initiate a password reset of all their affected accounts, particularly if they share passwords across multiple sites.<br>• Decommissioned the database at issue and retained forensic investigators to investigate the incident.<br>• Reviewing existing procedures and processes to minimize the likelihood of a similar event occurring in the future. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by email on October 8, 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 reported "Personal contact information can be used in misconduct such as spam and phishing".<br><br>In my view, a reasonable person would consider that the information at issue could be used for phishing purposes and to compromise other online accounts, increasing vulnerability to identity theft and fraud. 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 the likelihood of harm resulting from this incident is "Unlikely. There is no indication that this information has been released, and no reason that this information in particular would be misused".<br><br>In my view, a reasonable person would consider the likelihood of harm resulting from this incident is reduced as the breach does not appear to be the result of malicious intent. However, the Organization does not appear to know how long the information was exposed, and did not provide any information concerning possible access to the information (i.e. audit logs?). |

| 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 information at issue could be used for phishing purposes and to compromise other online accounts, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm is reduced as the breach does not appear to be the result of malicious intent. However, the Organization does not appear to know how long the information was exposed, and did not provide any information concerning possible access to the information (i.e. audit logs?).<br><br>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).<br><br>I understand individuals were notified by email on October 8, 2019. The Organization is not required to notify affected individuals again. |

Jill Clayton
Information and Privacy Commissioner