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** | The Living Desert (Organization) |
| **Decision number (file number)** | P2019-ND-158 (File #013158) |
| **Date notice received by OIPC** | April 23, 2019 |
| **Date Organization last provided information** | September 24, 2019 |
| **Date of decision** | October 24, 2019 |
| **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 located in Palm Desert, California USA and 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>• address, and<br>• payment card data.<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 personal information was collected in Alberta, PIPA applies. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |
| **Description of incident** | • On February 4, 2019, a computer forensics firm hired by the Organization reported that a limited number of the Organization's employee email accounts may have been accessed without authorization, and certain accounts may have contained personal information. |

| | |
|---|---|
| | • On February 13, 2019, the Organization engaged a document review vendor to search the contents of those email accounts for personal information.<br>• On March 6, 2019, the Organization learned that information of seventeen Canadians (including 4 Albertans) was contained within the employee email accounts.<br>• The Organization said it was not aware of any misuse of the information as a result of the incident. |
| **Affected individuals** | The incident affected four (4) Alberta residents. |
| **Steps taken to reduce risk of harm to individuals** | • Working with leading cybersecurity experts to ensure its digital environment is secure.<br>• Notified the Federal Bureau of Investigation (FBI).<br>• Notified affected individuals and provided information on how to protect their personal information.<br>• Consulted legal counsel as to notification requirements.<br>• Notified appropriate data protection authorities. |
| **Steps taken to notify individuals of the incident** | The affected individuals in Alberta were notified by letter sent on June 4, 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 included a document called "*Steps You Can Take to Further Protect Your Information"* and includes instruction on how to place a fraud alert on a credit report.<br><br>In my view, a reasonable person would consider that the contact (name and address) and financial information (payment card information) at issue could be used to cause the harms of identity theft and fraud. |
| **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 assess the likelihood that significant harm would result from this incident, but reported that "it was not aware of any misuse of the information as a result of the incident."<br><br>In my view, a reasonable person would consider that 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 into an employee's email account). The Organization reported that it was not aware of any misuse of the information as a result of the incident; however, the potential harms of identity theft and fraud can occur months or even years after personal information is |

| | |
|---|---|
| | compromised. Further, it appears that the information may have been exposed for approximately 6 weeks. |

**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 contact (name and address) and financial information (payment card information) at issue could be used to cause the harms of identity theft and fraud. 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 into an employee's email account). The Organization reported that it was not aware of any misuse of the information as a result of the incident; however, the potential harms of identity theft and fraud can occur months or even years after personal information is compromised. Further, it appears that the information may have been exposed for approximately 6 weeks.

I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individuals by letter sent on June 4, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner