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** | Kingdom Animalia LLC d.b.a. Hourglass Cosmetics (Organization) |
| **Decision number (file number)** | P2019-ND-073 (File #012080) |
| **Date notice received by OIPC** | February 19, 2019 |
| **Date Organization last provided information** | February 19, 2019 |
| **Date of decision** | June 3, 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 an "organization" as defined in section 1(1)(i) of PIPA. |
| **Section 1(1)(k) of PIPA "personal information"** | The incident involved the following information:<br><br>• name,<br>• address,<br>• email address,<br>• telephone number,<br>• product purchase details, and<br>• credit card number, CCV, and expiry date (if provided by the customer during the online checkout process for purchases between July 3, 2018 and January 30, 2019).<br><br>This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |

| | |
|---|---|
| Description of incident | • After learning of a potential issue with its online e-commerce website (www.hourglasscosmetics.com), the Organization conducted an investigation.<br>• The investigation determined that, from approximately July 3, 2018 to January 30, 2019, unauthorized third parties had the ability to access information of customers who had made a purchase on the site. |
| **Affected individuals** | The incident affected 168 Canadians, including 19 Alberta residents. |
| **Steps taken to reduce risk of harm to individuals** | • Conducted an investigation with the assistance of external cybersecurity experts.<br>• Removed the code that facilitated the unauthorized scraping of data during the check-out process and to prevent further access to the database.<br>• Undertook a review of patching and multiple security scans at the site and server level.<br>• Transitioning the site to a new platform.<br>• Reported the breach to law enforcement and its payment processor. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by letter on February 15, 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 harm(s) that might result from this incident, but its notice to affected individuals encouraged them to take precautions against "threats of identity theft or fraud" and to "Be alert for 'phishing' emails".<br><br>In my view, a reasonable person would consider that the contact, financial and transaction information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, 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 did not specifically assess the likelihood of harm resulting from this breach.<br><br>In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the incident is the result of malicious intent (deliberate intrusion). It appears the information may have been exposed for almost 7 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, financial and transaction information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.<br><br>The likelihood of harm resulting from this incident is increased as the incident is the result of malicious intent (deliberate intrusion). It appears the information may have been exposed for almost 7 months.<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 that affected individuals were notified by letter on February 15, 2019. The Organization is not required to notify the affected individuals again. |

Jill Clayton
Information and Privacy Commissioner