



**PERSONAL INFORMATION PROTECTION ACT**  
**Breach Notification Decision**

<b>Organization providing notice under section 34.1 of PIPA</b>	Victoria's Secret Store Brand Management, LLC (Organization)
<b>Decision number (file number)</b>	P2021-ND-019 (File #016496)
<b>Date notice received by OIPC</b>	July 21, 2020
<b>Date Organization last provided information</b>	July 21, 2020
<b>Date of decision</b>	February 23, 2021
<b>Summary of decision</b>	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 <i>Personal Information Protection Act</i> (PIPA).
<b>JURISDICTION</b>	
<b>Section 1(1)(i) of PIPA "organization"</b>	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
<b>Section 1(1)(k) of PIPA "personal information"</b>	<p>The Organization reported the incident involved the following information:</p> <ul style="list-style-type: none"><li>• name,</li><li>• postal address (if entered),</li><li>• email address,</li><li>• birth day and month (not year),</li><li>• telephone number,</li><li>• payment card information (if saved, only last four digits of the payment card).</li></ul> <p>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.</p>
<b>DESCRIPTION OF INCIDENT</b>	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	

<b>Description of incident</b>	<ul style="list-style-type: none"> <li>• The Organization learned that an unauthorized individual gained access to personal information in certain of its online accounts from approximately April 28, 2020 to May 13, 2020.</li> <li>• The Organization believes that the individual capitalized on a breach of another company’s system where the customer may have used the same login information.</li> </ul>
<b>Affected individuals</b>	The incident affected four (4) residents of Alberta.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>• Took steps to secure the accounts and determine the nature of the issue.</li> <li>• Coordinating with law enforcement authorities.</li> <li>• Informed affected individuals to change their current password and create a new one.</li> <li>• Informed affected individuals to monitor their online account for suspicious activity.</li> <li>• Informed affected individuals to change the username and password for all other online accounts for which they use the same or similar username and password.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	Affected individuals were notified of the incident on July 20, 2020.
<b>REAL RISK OF SIGNIFICANT HARM ANALYSIS</b>	
<p><b>Harm</b> 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.</p>	<p>The Organization did not specifically provide an assessment of the harm(s) that might result from this incident. However, in its notice to affected individuals, the Organization said,</p> <p style="text-align: center;"><i>Please monitor your ... online account for suspicious activity. Promptly change the username and password for all other online accounts for which you use the same or similar username and password.</i></p> <p>In my view, a reasonable person would consider that the contact, financial and partial identity information, particularly in combination, could be used for the purposes of identity theft and fraud. Email address could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms.</p>
<p><b>Real Risk</b> The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship</p>	<p>The Organization did not specifically provide an assessment of the likelihood that significant harm would result from this incident.</p> <p>In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion.</p>

between the incident and the possible harm.	The personal information may have been exposed for approximately two weeks.
<b>DECISION UNDER SECTION 37.1(1) OF PIPA</b>	
<p>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.</p> <p>A reasonable person would consider that the contact, financial and partial identity information, particularly in combination, could be used for the purposes of identity theft and fraud. Email address could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms.</p> <p>The likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion. The personal information may have been exposed for approximately two weeks.</p> <p>I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the Organization notified the affected individuals on July 20, 2020 in accordance with the <i>Regulation</i>. The Organization is not required to notify the affected individuals again.</p>	

Jill Clayton  
Information and Privacy Commissioner