



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

<b>Organization providing notice under section 34.1 of PIPA</b>	PetSmart, Inc. (Organization)
<b>Decision number (file number)</b>	P2019-ND-007 (File #009840)
<b>Date notice received by OIPC</b>	September 24, 2018
<b>Date Organization last provided information</b>	September 24, 2018
<b>Date of decision</b>	January 3, 2019
<b>Summary of decision</b>	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
<b>JURISDICTION</b>	
<b>Section 1(1)(i) of PIPA “organization”</b>	The Organization operates in Alberta and is an “organization” as defined in section 1(1)(i) of PIPA.
<b>Section 1(1)(k) of PIPA “personal information”</b>	<p>The incident involved the following information:</p> <ul style="list-style-type: none"><li>• telephone number,</li><li>• selection of pet preference depicted on the site,</li><li>• email address (in the case of two customers).</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 this 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’s third-party vendor hosts a website allowing customers to enrol to receive text messages (<a href="http://petsmartmobile.hit2c.com/us/join">http://petsmartmobile.hit2c.com/us/join</a>).</li><li>• The website encountered a vulnerability that allowed unauthorized access to telephone numbers of customers that were identified as Alberta residents, between August 12-16, 2018.</li></ul>

	<ul style="list-style-type: none"> <li>• The vendor addressed the issue on August 16, 2018 ensuring the website's security. This incident did not impact any other of the Organization's websites or e-commerce platforms.</li> <li>• The incident affected individuals (customers) that enrolled to receive text messages from the Organization and who entered their telephone number on the affected site on or before August 16, 2018.</li> </ul>
<b>Affected individuals</b>	The incident affected 1,030 residents of Alberta.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>• The vendor immediately took measures to address the technical issue that allowed the unknown threat actor to gain unauthorized access to the site.</li> <li>• Will ensure that contractual provisions with respect to safeguarding continue to be applied and has reiterated to the vendor the importance of safeguarding the Organization's customer personal information.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	Affected customers residing in Alberta were notified by letter.
<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 identify any potential harms that might result from this incident but its notification to affected individuals said "Access to your phone number can leave you at risk of phishing attempts or phone scams, where individuals try to collect other personal or financial data. Therefore, we recommend that you remain alert for suspicious communications or marketing campaigns from third parties that reference your phone number or interaction with [the Organization]."</p> <p>I agree with the Organization that a reasonable person would consider that the telephone number, profile information (customer of the Organization), and email address, could be used for targeted phishing purposes. Previous breach notification decisions issued by my office have found phishing to be a significant harm.</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 between the incident and the possible harm.</p>	<p>The Organization did not specifically assess the likelihood of harm resulting from this incident.</p> <p>In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent (deliberate action by an unauthorized party). The information was exposed for four days.</p>

**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 telephone number, profile information (customer of the Organization), and email address, could be used for targeted phishing purposes. Previous breach notification decisions issued by my office have found phishing to be a significant harm. The likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent (deliberate action by an unauthorized party). The information was exposed for four days.

I require the Organization to notify the affected individuals whose 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. The Organization is not required to notify the affected individuals again.

Jill Clayton  
Information and Privacy Commissioner