



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

<b>Organization providing notice under section 34.1 of PIPA</b>	Thirty-One Gifts Canada Inc. (Organization)
<b>Decision number (file number)</b>	P2017-ND-149 (File 005527)
<b>Date notice received by OIPC</b>	May 11, 2017
<b>Date Organization last provided information</b>	May 11, 2017
<b>Date of decision</b>	November 8, 2017
<b>Summary of decision</b>	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual 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 incident involved all or some of the following information:</p> <ul style="list-style-type: none"><li>• name,</li><li>• shipping address, and</li><li>• payment card account number.</li></ul> <p>This information is about an identifiable individual and is “personal information” as defined in section 1(1)(k) of PIPA. The information was collected from Albertans via the Organization’s website.</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>• On April 10, 2017, the Organization learned that a cyber intruder accessed an employee’s email account.</li><li>• The email account contained documents with portions of personal information.</li><li>• The Organization is unable to confirm that the information was in fact stolen.</li></ul>

	<ul style="list-style-type: none"> <li>The incident occurred between April 8, 2017 and April 10, 2017.</li> </ul>
<b>Affected individuals</b>	The incident affected twenty-six (26) individuals, including one (1) Alberta resident.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>Immediately took steps to block access.</li> <li>Secured other employee email accounts.</li> <li>Reviewed policy and procedures in light of this incident for areas of improvement.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	The affected individual was notified by letter sent on April 28, 2017.
<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 directly address the possible harm that might result from this incident, but reported “There is no evidence at this time that any personal information was in fact stolen as a result of this incident” and “Additionally, sensitive authentication data like card verification codes and PINs were not involved, making it unlikely that fraudulent payment card transactions can be completed.” The Organization’s notification letter to affected individuals recommended “that you review the information provided in this letter for some steps that you may take to protect yourself against any potential misuse of your personal information.”</p> <p>In my view, the contact and financial information at issue could be used for identity theft and fraud purposes. These are 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 between the incident and the possible harm.</p>	<p>The Organization reported that “it is unlikely that significant harm could result... there is only an indication that the intruder accessed an email account that had emails containing portions of information pertaining to one individual at a time...sensitive authentication data like credit card verification codes and PINs were not involved, making it unlikely that fraudulent payment card transactions can be completed... [the Organization] has not confirmed that any information was in fact viewed or stolen on this incident.”</p> <p>In my view, 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). Further, the information was exposed for two days and the Organization is unable to confirm the information in the email account accessed by the intruder was not viewed or stolen.</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 individual.

The contact and financial information at issue could be used for identity theft and fraud purposes. These are significant harms. 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). Further, the information was exposed for two days and the Organization is unable to confirm the information in the email account accessed by the intruder was not viewed or stolen.

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

I understand the Organization notified the affected individual in a letter dated April 28, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton  
Information and Privacy Commissioner