



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

<b>Organization providing notice under section 34.1 of PIPA</b>	Best Buy Canada Inc. (Organization)
<b>Decision number (file number)</b>	P2016-ND-32 (File #000198)
<b>Date notice received by OIPC</b>	January 23, 2015
<b>Date Organization last provided information</b>	February 5, 2015
<b>Date of decision</b>	May 30, 2016
<b>Summary of decision</b>	<p>There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).</p>
<b>JURISDICTION</b>	
<b>Section 1(1)(i) of PIPA “organization”</b>	The Organization is incorporated 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>• name,</li><li>• email address,</li><li>• address,</li><li>• survey responses.</li></ul> <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.</p>
<b>DESCRIPTION OF INCIDENT</b>	
<p><input type="checkbox"/> loss      <input type="checkbox"/> unauthorized access      <input checked="" type="checkbox"/> unauthorized disclosure</p>	

<b>Description of incident</b>	<ul style="list-style-type: none"> <li>The Organization launched a consumer panel recruitment survey on January 19, 2015.</li> <li>Due to a flaw in the survey application, when a customer clicked on the URL link to fill out the survey, the customer found the survey was already pre-populated with responses provided by another individual.</li> <li>Customers completing the survey reported the incident to the Organization. Fourteen customers contacted the Organization to report the issue.</li> <li>The Organization reported that the survey was mistakenly launched in the test environment instead of production environment – the link to the survey led to the test environment.</li> <li>The Organization reported that 4,090 customers started the survey; 1,371 actually completed it and submitted it to the Organization.</li> <li>The personal information was exposed for approximately 2 hours before the survey was taken down.</li> </ul>
<b>Affected individuals</b>	There were 1,371 affected individuals.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>The survey was shut down within two hours of the incident.</li> <li>The incident was investigated.</li> <li>The Organization obtained confirmation from the survey provider company that its employees had completed privacy compliance training.</li> <li>The Organization took steps to ensure quality assurance and approval of the survey prior to redeployment.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	Affected individuals were notified by email on January 23, 2015.
<b>REAL RISK OF SIGNIFICANT HARM ANALYSIS</b>	
<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>The Organization did not specifically identify any harm that might result from this incident, but reported that it believed “the risk of harm to our customers is low.”</p> <p>In my view, the contact information involved in this incident, in conjunction with the survey responses, provides a comprehensive profile of each affected individual which could be used to cause the harms of identity theft or fraud. Further, email addresses could be used to cause the harm of phishing. These are significant harms.</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.	The Organization reported that it believed “the risk of harm to our customers is low”.  In my view, despite the fact this incident resulted from human error and not malicious intent, and the information was exposed for a relatively short period of time, the likelihood of harm resulting is increased because of the number of exposures. That is, it appears at least 1,371 customers had unauthorized access to another individual’s personal information.
--	--

#### **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. The contact information involved in this incident, in conjunction with the survey responses, provides a comprehensive profile of each affected individual which could be used to cause the significant harms of identity theft or fraud. Further, email addresses could be used to cause the significant harm of phishing. Despite the fact this incident resulted from human error and not malicious intent, and the information was exposed for a relatively short period of time, the likelihood of harm resulting is increased because of the number of exposures.

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

I understand the Organization notified the affected individuals on January 23, 2015 in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton  
Information and Privacy Commissioner