



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

<b>Organization providing notice under section 34.1 of PIPA</b>	Best Buy Canada Ltd. (Organization)
<b>Decision number (file number)</b>	P2021-ND-102 (File #012998)
<b>Date notice received by OIPC</b>	April 10, 2019
<b>Date Organization last provided information</b>	April 10, 2019
<b>Date of decision</b>	March 31, 2021
<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>	The Organization reported that the personal information at issue is “Unknown”.  To the extent this incident involves information about identifiable individuals, it qualifies as “personal information” as defined in section 1(1)(k) of PIPA.
<b>DESCRIPTION OF INCIDENT</b>	
<input checked="" type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
<b>Description of incident</b>	<ul style="list-style-type: none"><li>• On or around March 31, 2019, a customer brought a computer to the Organization for repair and a data backup service. A sign in form was completed.</li><li>• The computer and form were sent to a service center; the computer was repaired and the data backup completed on a SSD card. The SSD card was subsequently lost and has not been recovered.</li><li>• The breach was discovered on April 2, 2019.</li></ul>

<b>Affected individuals</b>	The incident affected 1 individual.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>• Offered to cover the cost of 12-months credit monitoring for the customer.</li> <li>• Recommended the customer change his password for any other accounts or devices where he might use a similar username and password.</li> <li>• Implemented a new procedure for handling hard drives/SSD cards.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	The affected individual was notified by letter on April 9, 2019.
<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 the type of harm(s) that might result from this incident but did say “If someone has access to the SSD card, they might have access to the customer's personal information”.</p> <p>In my view, a reasonable person would consider that the type of personal information commonly stored on a personal computer could be used to cause multiple harms, including fraud and identity theft. 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 “The Service Center determined that the SSD card could have been either sent to recycling as per our procedure or included with another customer's shipment by error. Since the SSD card can not be found, it is possible that someone could have access to the personal information of the customer and fraudulently used the personal information of the Customer to create harm”.</p> <p>The Organization also said that “...the data, located on the SSD card, would not be immediately accessible, a special adapter with an Apple computer or Windows PC with special software to read Apple drives would be required to access the personal information.”</p> <p>In my view, a reasonable person would consider the likelihood of significant harm resulting in this case is increased because the Organization does not know the cause (theft or misplaced/lost), and the information has not been recovered. Although the information “would not be immediately accessible”, the Organization also said “it is possible that someone could have access to the personal information of the customer”.</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.

A reasonable person would consider that the type of personal information commonly stored on a personal computer could be used to cause multiple harms, including fraud and identity theft. These are significant harms.

The likelihood of significant harm resulting in this case is increased because the Organization does not know the cause (theft or misplaced/lost), and the information has not been recovered. Although the information “would not be immediately accessible”, the Organization also said “it is possible that someone could have access to the personal information of the customer”.

The Organization is required to notify the affected individual in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the affected individual was notified by letter on April 9, 2019. The Organization is not required to notify the affected individual again.

Jill Clayton  
Information and Privacy Commissioner