



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

<b>Organization providing notice under section 34.1 of PIPA</b>	Prudent Benefits Administration Services Inc. (the Organization)
<b>Decision number (file number)</b>	P2019-ND-076 (File #011955)
<b>Date notice received by OIPC</b>	February 5, 2019
<b>Date Organization last provided information</b>	February 5, 2019
<b>Date of decision</b>	June 4, 2019
<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 those 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 incident involved all or some of the following information:</p> <ul style="list-style-type: none"><li>• name,</li><li>• date of birth,</li><li>• address,</li><li>• security question,</li><li>• email address,</li><li>• telephone number,</li><li>• plan number,</li><li>• member ID,</li><li>• dependant information (name, date of birth, relationship, gender),</li><li>• beneficiary information (name, date of birth, relationship),</li><li>• benefit claims history.</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 information was collected in Alberta, PIPA applies.</p>

<b>DESCRIPTION OF INCIDENT</b>	
<input type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure	
<b>Description of incident</b>	<ul style="list-style-type: none"> <li>• The Organization is a third party administration firm and was creating portals for clients. During the process, the website was populated with the wrong certificate numbers which allowed some individuals to see personal information of a fellow union member.</li> <li>• The incident occurred between December 27, 2018 and January 7, 2019.</li> <li>• The incident was discovered on January 4, 2019 when a member contacted the Organization to report she accessed the portal and could see another person's information.</li> </ul>
<b>Affected individuals</b>	The incident affected 13 individuals, fewer than 8 of whom were Alberta residents.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>• Shut down the portals while assessing the incident.</li> <li>• Reviewed files for accuracy.</li> <li>• The Organization's IT team, in consultation with administrators, have reviewed the remaining accounts to ensure all data is correct and matched to the right individuals.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	Affected individuals were notified by letter the week of January 14, 2019.
<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(s) that might result from the breach.</p> <p>In my view, a reasonable person would consider the contact, identity and insurance information at issue could be used to cause the significant harms of identity theft and fraud.</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>The Organization did not specifically assess the likelihood of harm resulting from this incident, but did report that, other than the original report of the problem, "... no one else has contacted our office to report any further incidents. No banking information was connected to any individual account."</p> <p>In my view, a reasonable person would consider that the likelihood of harm is reduced because the breach did not result from malicious intent. Nonetheless, it is not clear from the Organization's report</p>

	<p>how many individuals may have accessed the information, nor any technical controls (such as audit logs) that could evidence that the information was not accessed. It appears the information was exposed for over a week.</p>
<p><b>DECISION UNDER SECTION 37.1(1) OF PIPA</b></p>	
<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 the contact, identity and insurance information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm is reduced because the breach did not result from malicious intent. Nonetheless, it is not clear from the Organization’s report how many individuals may have accessed the information, nor any technical controls (such as audit logs) that could evidence that the information was not accessed. It appears the information was exposed for over a week.</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 affected individuals were notified by letter the week of January 14, 2019. The Organization is not required to notify the affected individuals again.</p>	

Jill Clayton  
Information and Privacy Commissioner