



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

<b>Organization providing notice under section 34.1 of PIPA</b>	Allstate Insurance Company of Canada (Organization)
<b>Decision number (file number)</b>	P2013-ND-39 (File #P2307)
<b>Date notice received by OIPC</b>	April 11, 2013
<b>Date Organization last provided information</b>	October 23, 2013
<b>Date of decision</b>	December 4, 2013
<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 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>	Organization is federally incorporated and licenced under the Alberta <i>Insurance Act</i> to carry on business in Alberta.  I have jurisdiction because the Organization is an “organization” as defined in section 1(1)(i)(i) of PIPA.
<b>Section 1(1)(k) of PIPA “personal information”</b>	The incident involved the following information for all individuals: <ul style="list-style-type: none"><li>• name,</li><li>• address,</li><li>• driver’s licence number,</li><li>• loss history (including previous accidents or policy violations),</li><li>• date of birth, and</li><li>• vehicle information and property information.</li></ul> In addition, the incident involved the following information for some of the individuals:

	<ul style="list-style-type: none"> <li>• bank account information (for four individuals), and</li> <li>• credit card number and expiry date (for ten individuals).</li> </ul> <p>This information is “personal information” as defined in section 1(1)(k) of PIPA and was collected in Alberta.</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>• An employee of the Organization created fictitious policies for the affected individuals in order to influence the employee’s work performance record.</li> <li>• There were 45 property policies and 33 auto policies created.</li> <li>• All policies were retracted by the employee except for three. These three policies were sent to a collection agency for failure to pay the policy. This was discovered during an internal investigation.</li> <li>• The insurance policies were created between 2012 and 2013.</li> </ul>
<b>Affected individuals</b>	78 individuals were affected, all of which were Alberta residents.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>• Reimbursement of financial losses to affected individuals.</li> <li>• Computer search of the employee’s files and emails conducted to verify personal information of the individuals was not stored elsewhere by the employee.</li> <li>• Contacted the collection agency and informed them that the information was sent in error.</li> <li>• Adjusted the affected individuals’ records so this incident will not be on their file when dealing with other insurance companies.</li> <li>• Offer to add a security question on affected individuals’ plan member file.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	Notification sent by mail to affected individuals between May 3 and May 10, 2013. The Organization also contacted each affected individual by phone during the same time period.
<b>REAL RISK OF SIGNIFICANT HARM ANALYSIS</b>	
<b>Harm</b> Some damage or detriment or injury – that could be caused	The Organization recognized the affected individuals may be at risk for financial loss as well as identity theft or fraud. This is particularly the case for the 14 individuals whose credit card

<p>to those 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>information or banking information was accessed. The Organization confirmed this information was used to bill the affected individuals for the fictitious policies.</p> <p>In my view, the personal information involved is sensitive. It contains identity information such as date of birth and, in 14 cases, credit card or banking information. The types of harm that could result from unauthorized access to the personal information in this instance are identity theft and fraud. In my view, 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 due to the personal information involved, it considered there to be a real risk of significant harm to the affected individuals. The risk materialized when the credit card and banking information of 14 of the affected individuals was used without authorization and when three of those 14 individuals had their personal information sent to a collection agency for non-payment.</p> <p>The Organization reported that the employee is no longer employed by the Organization but it cannot be ruled out that the employee did not record the information obtained prior to leaving the Organization.</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. The personal information involves sensitive identity information, such as date of birth for all affected individuals, and financial information for 14 individuals. These factors contributed significantly to my decision.</p> <p>I require the Organization to notify the affected individuals in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the Organization notified the affected individuals via telephone and mail between May 3, 2013 and May 10, 2013, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.</p>	

Jill Clayton  
Information and Privacy Commissioner