



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

<b>Organization providing notice under section 34.1 of PIPA</b>	Alberta Treasury Branches, carrying on business as ATB Financial (Organization)
<b>Decision number (file number)</b>	P2013-ND-40 (File #P2386)
<b>Date notice received by OIPC</b>	July 16, 2013
<b>Date Organization last provided information</b>	July 16, 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>	The Organization is incorporated in Alberta.  I have jurisdiction because 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 incident involved all or some of the following information: <ul style="list-style-type: none"><li>• name,</li><li>• account number, and</li><li>• account balance.</li></ul> This information is “personal information” as defined in section 1(1)(k) of PIPA and was collected from Alberta residents.
<b>DESCRIPTION OF INCIDENT</b>	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	

<p><b>Description of incident</b></p>	<ul style="list-style-type: none"> <li>• On the night of June 15, 2013 the Organization’s Marwayne Agency located in Marwayne, AB, was broken into and the safe stolen.</li> <li>• The safe contained a rolodex and a hard drive which contained unencrypted personal information belonging to 123 individuals.</li> <li>• The safe was later found but the rolodex and hard drive were missing.</li> <li>• Personal information on the rolodex included clients’ name and account number.</li> <li>• Personal information stored on the hard drive included clients’ name, account number and balance, and general email correspondence between the branch and ATB Agent (which may have included client name and account number).</li> </ul>
<p><b>Affected individuals</b></p>	<p>123 customers who are all Alberta residents.</p>
<p><b>Steps taken to reduce risk of harm to individuals</b></p>	<ul style="list-style-type: none"> <li>• The Organization immediately notified the RCMP of the incident.</li> <li>• Placed notes on the affected individuals’ accounts and is monitoring them for any unauthorized activity.</li> <li>• Offered to close accounts and open new accounts for the affected individuals.</li> <li>• Offered free credit monitoring for the affected individuals.</li> </ul>
<p><b>Steps taken to notify individuals of the incident</b></p>	<p>A notification letter was mailed to all affected individuals the week of June 24-28, 2013.</p>
<p><b>REAL RISK OF SIGNIFICANT HARM ANALYSIS</b></p>	
<p><b>Harm</b> Some damage or detriment or injury – that could be caused 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>The Organization recognized the affected individuals may be at risk for identity theft and fraud.</p> <p>In this case, the personal information at issue consists of individual’s names, account number and account balance. While an individual’s name is not particularly sensitive information, the inclusion of the account number in connection with this information raises the sensitivity of the information to moderate to high sensitivity.</p> <p>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 circumstances (theft) and sensitivity of the personal information involved, it considered there to be a real risk of significant harm to the affected individuals.</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the personal information was stolen and has not been recovered.</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 individuals. The personal information involves sensitive information, such as name and account number. The information was stolen and has not been recovered. The circumstances and personal information involved are similar to the circumstances and personal information reported by the Organization to me in P2010-ND-006 and P2011-ND-005. In both of those cases, I determined there to be a real risk of significant harm to the affected individuals. These factors contributed significantly to my decision.

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 in accordance with the Regulation in a letter that was sent between June 24-28, 2013. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton  
Information and Privacy Commissioner