



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

<b>Organization providing notice under section 34.1 of PIPA</b>	Southern Michigan Bank & Trust (Organization)
<b>Decision number (file number)</b>	P2017-ND-70 (File #002986 )
<b>Date notice received by OIPC</b>	May 25, 2016
<b>Date Organization last provided information</b>	June 23, 2016
<b>Date of decision</b>	June 7, 2017
<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’s principal place of business is Michigan, United States. It is an “organization” as defined in section 1(1)(i)(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>• address,</li><li>• date of birth,</li><li>• Social Insurance Number (SIN),</li><li>• bank account information,</li><li>• employee identification number,</li><li>• driver’s licence number, and</li><li>• tax identification number.</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 from individuals residing in Alberta at the time their accounts were opened.</p>
<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 April 10, 2016, a vehicle belonging to an employee of the Organization was burglarized in the United States. A company laptop containing personal information of customers was stolen.</li> <li>The laptop was password protected but not encrypted.</li> <li>The laptop has not been recovered to date.</li> </ul>
<b>Affected individuals</b>	The incident affected three (3) residents of Alberta.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>Retained a third party forensic investigator.</li> <li>Reported the incident to local law enforcement.</li> <li>Provided complimentary access to 12 months of services such as credit and identity monitoring, identity consultation and restoration services.</li> <li>Provided information to affected individuals on how to protect against identity theft and fraud.</li> <li>Provided notice of the incident to state and federal regulators and consumer reporting agencies.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	Affected individuals were notified by mail on May 9, 2016.
<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.	The Organization did not identify any specific harms that might result from this incident but reported that it was “providing individuals and businesses impacted by this incident with helpful information on how to protect against identity theft and fraud.”  I agree with the Organization. The information at issue includes contact, identity, financial and employment information that could be used to cause the harms of identity theft, fraud and financial loss. These are significant harms.
<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 did not report its assessment of the likelihood of harm resulting from this incident, but in its notice to potentially affected individuals it said it was “unaware of any actual or attempted misuse of information potentially stored on the laptop at the time of the theft.” The Organization offered credit and identity monitoring to affected individuals.  In my view, the likelihood of harm resulting from this incident is increased because the laptop was stolen, indicating malicious intent. The laptop was not encrypted and has not been recovered.

**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 information at issue includes contact, identity, financial and employment information that could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm resulting from this incident is increased because the laptop was stolen, indicating malicious intent. The laptop was not encrypted and has not been recovered.

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

I understand the Organization notified affected individuals by mail on May 9, 2016, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton  
Information and Privacy Commissioner