



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

<b>Organization providing notice under section 34.1 of PIPA</b>	Baker Funeral Chapel Inc. (Organization)
<b>Decision number (file number)</b>	P2021-ND-264 (File #020722)
<b>Date notice received by OIPC</b>	April 23, 2021
<b>Date Organization last provided information</b>	April 23, 2021
<b>Date of decision</b>	February 9, 2022
<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 operates in Alberta and 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>• telephone number,</li><li>• address of next of kin of deceased, and</li><li>• vital statistic information of the deceased.</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 the information was collected in Alberta, PIPA applies.</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>• On April 21, 2021, the Organization was subject to a ransom attack, which encrypted its network system.</li><li>• The cyber-criminal asked for a bitcoin payment in order to obtain a key to unlock the system.</li></ul>

	<ul style="list-style-type: none"> <li>• The affected files included templates for funeral bulletins and obituaries that have been published in newspapers.</li> <li>• The Organization believes the breach occurred due to an invoice attachment that came in an email.</li> <li>• On April 22, 2021, the Organization reported that all computers were scanned on the premises and found no further threat.</li> </ul>
<b>Affected individuals</b>	The incident affected 7 individuals whose information was collected in Alberta.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>• Powered down all computers and unplugged all internet connections.</li> <li>• Changed all passwords.</li> <li>• Added further security measures.</li> <li>• Suspended Wifi.</li> <li>• Contacted local RCMP.</li> <li>• Notified Privacy Commissioner of Canada</li> <li>• Web browser cleared and changed.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	Affected individuals were contacted in in person or by telephone on April 22, 2021 and April 23, 2021.
<b>REAL RISK OF SIGNIFICANT HARM ANALYSIS</b>	
<p><b>Harm</b></p> <p>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 any harms that might result from this incident, but the Organization informed affected individuals,</p> <p style="text-align: center;"><i>Any emails from [the Organization] open with caution. [The Organization] will never require you to download an attachment asking for a password. No financial or banking information was stored on [the Organization’s] devices.</i></p> <p>It appears from this notice that the Organization is cautioning affected individuals about the possibility they may receive phishing emails. Given this, I accept that a reasonable person would consider the information at issue could be used to cause the significant harms of identity theft and fraud.</p>
<p><b>Real Risk</b></p> <p>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 did not specifically provide an assessment of the likelihood that significant harm would result from this incident.</p> <p>In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion, ransom demand).</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.

A reasonable person would consider the information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion, ransom demand).

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

I understand the Organization notified affected individuals in person and by telephone on April 22, 2021 and April 23, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton  
Information and Privacy Commissioner