



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

<b>Organization providing notice under section 34.1 of PIPA</b>	United on Whyte Pastoral Charge (Organization)
<b>Decision number (file number)</b>	P2017-ND-46 (File #002269)
<b>Date notice received by OIPC</b>	February 2, 2016
<b>Date Organization last provided information</b>	January 20, 2017
<b>Date of decision</b>	March 9, 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 is established under the federal <i>United Church of Canada Act</i> . I have jurisdiction because the Organization is an “organization” as defined in section 1(1)(i)(ii) of PIPA.
<b>Section 1(1)(k) of PIPA “personal information”</b>	<p>The following information was involved in this incident:</p> <ul style="list-style-type: none"><li>• name,</li><li>• address,</li><li>• telephone number,</li><li>• email address,</li><li>• church hall rental contracts.</li></ul> <p>Some or all of this information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.</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>• Between December 20, 2015 and December 22, 2015, the Organization experienced a break-in and a laptop computer was stolen from a locked office.</li></ul>

	<ul style="list-style-type: none"> <li>• The information at issue was stored on the laptop, which was password protected but not encrypted.</li> <li>• The laptop has not been recovered.</li> </ul>
<b>Affected individuals</b>	The incident affected approximately 125 individuals (including members of the congregation and individuals who had entered into contracts for renting the church hall).
<b>Steps taken to reduce risk of harm to individuals</b>	Reported incident to Edmonton Police Service on December 22, 2015.
<b>Steps taken to notify individuals of the incident</b>	Affected individuals have not been notified.
<b>REAL RISK OF SIGNIFICANT HARM ANALYSIS</b>	
<p><b>Harm</b> Some damage or detriment or injury that could be caused to the 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 reported “The types of harm that may result of [sic] the breach are as follows:</p> <ul style="list-style-type: none"> <li>• Fraud</li> <li>• Identity theft</li> <li>• Damage to or loss of property of congregation members because thief/thieves now know where members live.”</li> </ul> <p>In my view, email addresses in conjunction with affected individuals’ known association with the Organization could be used to profile and target affected individuals through phishing. This is a significant harm.</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 “It appeared, by the damage to the building, the thief or thieves were looking for money or items that were “pawnable.” The EPS agreed with this conclusion.” The Organization also noted that files in the office were not disturbed, the congregation is comprised mostly of senior citizens, and the laptop was setup so as to notify the Organization in the event it was used to access the internet. The Organization has not received any such notification.</p> <p>In my view, the risk of harm is increased because the incident resulted from malicious intent (break-in and theft of laptop), the laptop was not encrypted and has not been recovered, and the affected individuals are mostly seniors and are therefore a vulnerable population.</p>
<b>DECISION UNDER SECTION 37.1(1) OF PIPA</b>	
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.	

Email addresses in conjunction with affected individuals' known association with the Organization could be used to profile and target affected individuals through phishing. This is a significant harm. The risk of harm is increased because the incident resulted from malicious intent (break-in and theft of laptop), the information has not been recovered, and the affected individuals are mostly seniors and are therefore a vulnerable population.

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

The Organization reported it may not be possible to notify individuals directly because the information concerning congregation members may be outdated (the database on the laptop originated in 2009), some members are deceased, and it does not have records concerning the rental contracts that were on the laptop.

If the Organization has current contact information for affected individuals, I require the Organization notify them directly.

For those the Organization does not have current contact information for, I believe indirect notification to affected individuals is reasonable under the circumstances. An oral notice or announcement to the congregation should be given over a 2 week period during congregation sermons. If the Organization has a newsletter or printed material available at sermons, a printed notice of the incident should be placed in it. If the Organization has a bulletin board in a communal space, a notice can be posted on this for a 2 week period.

I require the Organization to provide me with written confirmation that it has notified affected individuals on or before April 7, 2017.

Jill Clayton  
Information and Privacy Commissioner