



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

<b>Organization providing notice under section 34.1 of PIPA</b>	Calder Bateman Communications Ltd. (Organization)
<b>Decision number (file number)</b>	P2019-ND-144 (File #006006)
<b>Date notice received by OIPC</b>	July 4, 2017
<b>Date Organization last provided information</b>	July 4, 2017
<b>Date of decision</b>	August 16, 2019
<b>Summary of decision</b>	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA), the Organization is required to notify the affected individuals.
<b>JURISDICTION</b>	
<b>Section 1(1)(i) of PIPA “organization”</b>	The Organization is incorporated and operating 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>• address,</li><li>• email address,</li><li>• telephone number.</li></ul> <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</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>• The Organization runs all aspects of the Caritas Dream life Lottery on behalf of the Covenant Foundation.</li><li>• On June 1, 2017, the Organization’s service provider, Pixel Army, discovered malware affected its system performance.</li><li>• The incident appears to be related to an earlier breach for which certain vulnerabilities remained undetected and unaddressed.</li></ul>



	<ul style="list-style-type: none"> <li>• The vulnerability affected transactions conducted through the Organization’s website between February 9 and 22, 2017.</li> <li>• The Organization and its service provider took steps to enhance information security and prevent reoccurrence.</li> </ul>
<b>Affected individuals</b>	The incident affected 38,334 individuals residing in Alberta.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>• Reported the incident to the Office of the Information and Privacy Commissioner of Alberta.</li> <li>• Reported the incident to law enforcement and the Alberta Gaming and Liquor Commission.</li> <li>• Revised protocol for storing transactional data.</li> <li>• Reviewed and enhanced cyber security.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	Affected individuals were notified by email on June 9, 2017.
<b>REAL RISK OF SIGNIFICANT HARM ANALYSIS</b>	
<p><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.</p>	<p>The Organization reported “The potential impact relates to identity theft” and also “A perpetrator could contact buyers under false pretences and try to obtain further information from the buyer.”</p> <p>In my view, a reasonable person would consider that the contact information at issue, and particularly email addresses, could be used for phishing purposes, increasing vulnerability to identity theft and fraud.</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:</p> <p style="text-align: center;"><i>We believe there was malicious intent.</i></p> <p style="text-align: center;"><i>In addition to the general risks associated with personal (but not credit) identity theft, there have been incidents involving other lotteries in Alberta, where the misuse of personal information specific to lotteries has included:</i></p> <ul style="list-style-type: none"> <li>• <i>Phishing incidents where people were directed to a false site which asked for credit card information.</i></li> <li>• <i>Phone calls to individuals - for example, claiming that the buyer had won a prize but needed to supply credit information in order to claim the prize.</i></li> </ul> <p>In my view, a reasonable person would consider that the likelihood of harm resulting from this breach is increased because it resulted from malicious intent (deliberate intrusion and malware).</p>

	<p>The information was exposed for almost 2 weeks. The Organization is aware of similar information being used for phishing purposes.</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.</p> <p>A reasonable person would consider that the contact information at issue, and particularly email addresses, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. The likelihood of harm resulting from this breach is increased because it resulted from malicious intent (deliberate intrusion and malware). The information was exposed for almost 2 weeks. The Organization is aware of similar information being used for phishing purposes.</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 affected individuals by email on June 9, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.</p>	

Jill Clayton  
Information and Privacy Commissioner