



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

<b>Organization providing notice under section 34.1 of PIPA</b>	Canadian Association of Petroleum Producers (Organization)
<b>Decision number (file number)</b>	P2016-ND-45 (File #002068)
<b>Date notice received by OIPC</b>	December 30, 2015
<b>Date Organization last provided information</b>	March 2, 2016
<b>Date of decision</b>	August 22, 2015
<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>	<p>The Organization is federally incorporated as a not-for-profit corporation.</p> <p>Section 56(3) limits the application of PIPA to personal information collected, used or disclosed by a “non-profit organization” in connection with a commercial activity.</p> <p>Although it operates on a not-for-profit basis, the Organization is not a “non-profit organization,” as defined by section 56(1)(b)(i) of PIPA.</p> <p>I have jurisdiction because the Organization is an “organization” as defined in section 1(1)(i)(i) of PIPA.</p>
<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>• position,</li><li>• date of hire,</li><li>• income,</li><li>• social insurance number,</li></ul>

	<ul style="list-style-type: none"> <li>• benefits and deductions,</li> <li>• bank account number (with only the last few digits shown),</li> <li>• employee identification number and other numeric codes (only used for internal purposes),</li> <li>• Record of Employment forms (includes name, social insurance number, date of hire, position, earnings, possibly address, start and end dates of employment).</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 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 December 24, 2015, a package sent by the Organization’s contracted payroll services provider, containing paper payroll data for the final pay period of the year, was stolen from a courier truck while it was making deliveries.</li> <li>• In March 2016, the Organization reported that it had been informed by its payroll service provider that “the bulk of the materials of concern have been recovered with some pages missing.”</li> </ul>
<b>Affected individuals</b>	There are approximately 95 affected individuals.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>• Contacted police.</li> <li>• Notified privacy officer and affected individuals.</li> <li>• Reviewing security and privacy issues with contracted payroll services provider.</li> <li>• Credit monitoring provided for a year to affected individuals.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	Affected individuals were originally notified by email on December 30, 2015 and updated on December 31, 2015. Another email was sent on March 1, 2016 after some of the materials were recovered.

**REAL RISK OF SIGNIFICANT HARM ANALYSIS**

<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 that its concern was mostly with identity theft, and the combination of Record of Employment with other personal information, including address. The Organization noted that bank account information was mostly “masked”, and also that there was the potential for embarrassment to result from the incident, depending on who might have access to the personal information.</p> <p>I agree with the Organization. The personal information at issue includes sensitive identity, financial and employment information that could be used to cause the harms of identity theft, fraud, financial loss, embarrassment and humiliation. 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>In assessing the likelihood of harm resulting from this incident, the Organization considered that the bank account information was mostly masked, it is likely that the thieves were looking for items like gift cards that could be readily cashed rather than personal information, and the incident was the result of malicious intent (theft). The Organization also reported that the materials were “partially recovered” and “no one has reported any inappropriate activity on their credit files.”</p> <p>In my view, the likelihood of harm resulting from this incident is increased because, while it may be that the thieves were looking for gift cards that could be readily cashed, this cannot be known for sure. The incident resulted from deliberate action (theft), indicating malicious intent, and the information has been only partially recovered after being exposed for some time. Further, although the bank account numbers were masked, this was not the case for other identity information such as social insurance numbers.</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 at issue includes sensitive identity, financial and employment information that could be used to cause the significant harms of identity theft, fraud, financial loss, embarrassment and humiliation. While it may be that the thieves were looking for gift cards that could be readily cashed, this cannot be known for sure. The incident resulted from deliberate action (theft), indicating malicious intent, and the information has been only partially recovered after being exposed for some time. Further, although the bank account numbers were masked, this was not the case for other identity information such as social insurance numbers.

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 by email on December 30, 2015 and received updated notifications on December 31, 2015 and again on March 1, 2016 after some of the materials were recovered. The Organization is not required to notify the affected individuals again.

Jill Clayton  
Information and Privacy Commissioner