



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

<b>Organization providing notice under section 34.1 of PIPA</b>	Open Text Corporation (Organization)
<b>Decision number (file number)</b>	P2017-ND-104 (File #006011)
<b>Date notice received by OIPC</b>	July 5, 2017
<b>Date Organization last provided information</b>	July 5, 2017
<b>Date of decision</b>	July 25, 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 the 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 an “organization” as defined in section 1(1)(i) of PIPA.
<b>Section 1(1)(k) of PIPA “personal information”</b>	<p>The following information may be at issue:</p> <ul style="list-style-type: none"><li>• name,</li><li>• date of birth,</li><li>• address,</li><li>• dates of employment,</li><li>• education history,</li><li>• salary,</li><li>• copy of Passport Bio page (including citizenship, place of birth, passport number),</li><li>• copies of old work permits,</li><li>• employee photograph,</li><li>• job description,</li><li>• letter of support from Organization (including job details of employment, resume, pay stubs, organizational charts).</li></ul> <p>This information is about identifiable individuals (current and former employees) and is “personal information” as defined in section 1(1)(k) of PIPA. Affected individuals include 2 residents of 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>On June 25, 2017, a storage device was stolen which may have contained personal information as of 2014 for current and former employees of the Organization.</li> <li>The Organization did not report recovering the storage device.</li> </ul>
<b>Affected individuals</b>	The incident affected approximately 300 employees, two (2) of whom are residents of Alberta.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>Reported incident to law enforcement.</li> <li>Offered affected individuals free identity theft protection services through a third-party provider.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	The Organization reported it would notify all affected Canadian residents beginning on June 30, 2017 and provided a copy of the notification with its report of the breach.
<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 reported that it “...considers that affected individuals could be at risk of identity theft or fraud as a result of this incident.”  I agree with the Organization. The comprehensive contact, identity and employment information at issue could be used to cause the harms of identity theft and fraud. 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.	As noted above, the Organization reported that it “...considers that affected individuals could be at risk of identity theft or fraud as a result of this incident.” The Organization also reported that it “...has received no information to suggest that the incident was anything other than an ordinary theft or that the data was itself targeted.”  In my view, the likelihood of harm in this case is increased because the incident resulted from malicious intent (theft of storage device) and the information has not been recovered. The Organization can only speculate that the information was not the intended target.

**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 comprehensive contact, identity and employment information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting in this case is increased because the incident resulted from malicious intent (theft of storage device) and the information has not been recovered. The Organization can only speculate that the information was not the intended target.

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 intended to notify all affected Canadian residents beginning on June 30, 2017. The Organization is not required to notify the affected individuals again, but is required to confirm to me on or before August 4, 2017 that notification took place.

Jill Clayton  
Information and Privacy Commissioner