



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

<b>Organization providing notice under section 34.1 of PIPA</b>	Connor, Clark & Lunn Private Capital Ltd. (Organization)
<b>Decision number (file number)</b>	P2022-ND-013 (File #022285)
<b>Date notice received by OIPC</b>	April 13, 2021
<b>Date Organization last provided information</b>	February 17, 2022
<b>Date of decision</b>	April 1, 2022
<b>Summary of decision</b>	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual 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’s head office is in Toronto, Ontario.  The Organization is an “organization” as defined in section 1(1)(i) of PIPA.
<b>Section 1(1)(k) of PIPA “personal information”</b>	The incident involved all or some of the following information: <ul style="list-style-type: none"><li>• name,</li><li>• address, and</li><li>• banking information.</li></ul> This information is about an identifiable individual and is “personal information” as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
<b>DESCRIPTION OF INCIDENT</b>	
<input type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure	
<b>Description of incident</b>	<ul style="list-style-type: none"><li>• On March 29, 2021, an email record search for a former client was sent to a wrong email address.</li><li>• On April 7, 2021, the Organization’s security team discovered the incident as part of their monitoring processes. They have confirmed no other emails have been sent to this email address.</li></ul>

<b>Affected individuals</b>	The incident affected one (1) individual.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>• Contacted the recipient and asked that the email sent in error be deleted.</li> <li>• Offered a complimentary six-month subscription to identity protection.</li> <li>• Confirmed no other emails have been sent to this email address.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	The affected individual was notified by letter sent on April 13, 2021.
<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 the possible harm that may occur as a result of the breach is “Identity theft”.  In my view, the contact and the banking information could be used to cause the harms of identity theft and fraud. Banking information could be used to cause financial loss. These are all 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.	The Organization reported,  <i>Low likelihood that identity theft will result. The email sent in error could be sent to the recipients [sic] junk mail. Furthermore, we are offering a complimentary six-month subscription to identity protection through Equifax Canada, which will alert the individual if there are any key changes to the Equifax credit report. A specialist will also be on hand who will provide assistance if there is any other impact arising from this situation.</i>  Although the unauthorized disclosure was caused by human error, in my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because it does not appear the Organization received confirmation that the email containing the affected individual’s personal information was deleted and not copied, forwarded or otherwise distributed.

**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 individual.

The contact and the banking information could be used to cause the harms of identity theft and fraud. Banking information could be used to cause financial loss. These are all significant harms.

The likelihood of harm resulting from this incident is increased because it does not appear the Organization received confirmation that the email containing the affected individual's personal information was deleted and not copied, forwarded or otherwise distributed.

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

I understand the Organization notified the affected individual in a letter on April 13, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Cara-Lynn Stelmack  
Assistant Information and Privacy Commissioner