



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

<b>Organization providing notice under section 34.1 of PIPA</b>	Grant Thornton Limited, acting as court-appointed Receiver for Western Precast Group Ltd. (Organization)
<b>Decision number (file number)</b>	P2018-ND-056 (File #008318)
<b>Date notice received by OIPC</b>	April 16, 2018
<b>Date Organization last provided information</b>	April 16, 2018
<b>Date of decision</b>	May 7, 2018
<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 an “organization” as defined in section 1(1)(i)(i) of PIPA.
<b>Section 1(1)(k) of PIPA “personal information”</b>	<p>The incident involved the following information:</p> <ul style="list-style-type: none"><li>• name,</li><li>• outstanding wages,</li><li>• vacation pay,</li><li>• termination pay, and</li><li>• social insurance number.</li></ul> <p>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 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>• The Organization prepared Wage Earner Protection Program Act (WEPPA) packages to be sent to former employees of Western Precast Group Ltd.</li></ul>

	<ul style="list-style-type: none"> <li>• Each package was to contain two documents: a letter regarding the WEPPA program and a personalized schedule which included the information at issue.</li> <li>• The schedules were prepared at a centralized processing centre.</li> <li>• An employee of the Organization was unaware that the schedules were personalized for each former employee and incorrectly assembled the packages without confirming that each schedule pertained to the correct recipient.</li> <li>• On February 25, 2018, the incorrectly assembled packages were mailed to former employees, some of whom received a schedule pertaining to another former employee. In some cases, the former employees may have received the correct schedule.</li> <li>• The incident was discovered on February 27, 2018 when the Organization started receiving calls from the former employees.</li> </ul>
<b>Affected individuals</b>	The incident affected 31 former employees.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>• Sought confirmation from each of the former employees that that they have not made use of, copied, saved, or further disseminated or disclosed the personal information and have destroyed or returned the information to the Organization.</li> <li>• Offered former employees free identity theft/credit monitoring for one year.</li> <li>• Prepared internal training related to the WEPPA program and all internal Edmonton staff completed it.</li> <li>• No longer includes social insurance numbers in WEPPA schedules.</li> <li>• Considering centralizing the preparation of all WEPPA packages across Canada so that the same specialized staff would be responsible for preparing all packages.</li> <li>• Considering implementing further privacy training programs.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	Affected individuals were notified in writing on April 3, 2018.
<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 that outstanding wages, vacation pay and termination pay “...would typically be of moderate sensitivity; however those pieces of personal information were already part of the public record as part of the ongoing receivership proceedings ... In any event, the SINs disclosed in the Incident are highly sensitive information”.</p> <p>The Organization further said that “the disclosure of the personal information ... in particular SINs could potentially be used to conduct identity theft and/or fraud. Additionally, as a result of the disclosure ... it is possible that the former...employees may suffer from</p>

	<p>embarrassment by having their outstanding wages, vacation pay, and termination pay disclosed to another former...employee”.</p> <p>I agree with the Organization. Although disclosure of the employment information at issue could be used to cause the harms of hurt, humiliation and embarrassment, the fact this information is part of the public record suggests that such harms would not (or would not necessarily) be the result of this incident. However, in conjunction with identity information (social insurance number), this information could be used to cause the significant harms of 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><i>The likelihood that harm may occur to any of the former ...employees is moderate. The Incident was an accident as a result of an administrative employee error and did not involve malicious intent on the part of any individual. Each former ... employee received the personal information for no more than one other former...employee.</i></p> <p><i>The [Organization] is aware of the identity of each of the former... employees who received personal information of other former ...employees and each former employee is similarly aware of the [Organization’s] knowledge of their identity. In all likelihood, each of the former employees also know the identity of each other which further reduces the possibility that any of the former ... employees would use the personal information for an improper purpose.</i></p> <p><i>As part of the Notification, the [Organization] has requested confirmation from each of the former...employees that no use has been made of the incorrect WEPPA Schedule or personal information contained therein, that the incorrect WEPPA Schedule they received or the information contained therein was not copied, saved, or further disseminated or disclosed, and that those former employees have either destroyed the incorrect WEPPA Schedule they received or returned it to the [Organization]. ...</i></p> <p><i>Following the Incident, one former... employee has indicated that they have been subject to an instance of identity theft. It is currently unknown whether the instance of identity theft complained of by the former ...employee is related to the Incident.</i></p>

	<p>In my view, there is a real risk of significant harm in this case, despite the fact the incident did not result from malicious intent (but rather a mailing error). The Organization took steps to confirm that the information at issue was not copied, saved, further disseminated or disclosed, and requested it be destroyed or returned; however, the Organization did not report whether it received such confirmation or returned information. One instance of identity theft has been complained of and may be related to this incident.</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, despite the fact the incident did not result from malicious intent (but rather a mailing error). The Organization took steps to confirm that the information at issue was not copied, saved, further disseminated or disclosed, and requested it be destroyed or returned; however, the Organization did not report whether it received such confirmation or returned information. One instance of identity theft has been complained of and may be related to this incident.

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

I understand that affected individuals were notified in writing on April 3, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton  
Information and Privacy Commissioner