



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Ledcor Construction Limited (Organization)
Decision number (file number)	P2018-ND-050 (File #008314)
Date notice received by OIPC	April 16, 2018
Date Organization last provided information	April 16, 2018
Date of decision	April 23, 2018
Summary of decision	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).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	The Organization is an “organization” as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	<p>The incident involved the following information:</p> <ul style="list-style-type: none">• name,• home address,• social insurance number,• annual income,• deductions (EI, CPP, RRSP contributions), and• information about charitable donations. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. The incident occurred in Edmonton and Calgary, Alberta.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• On February 28, 2018, the Organization provided T4 forms to 44 employees/ex-employees. Inadvertently, the recipients received their own T4, as well as information about another employee/ex-employee.

	<ul style="list-style-type: none"> • The error was the result of the Organization providing an incorrect file to its third party provider, who was responsible for distributing the T4 forms. The mistake was not picked up by the third-party provider. • The incident was discovered on March 6, 2018, when employees who received the incorrect T4s reported the matter to their supervisors, who reported it to payroll.
Affected individuals	The incident affected 44 individuals.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Requested unauthorized recipients return the paper records and acknowledge that they did not make or retain any copies, and have not used and will not use the information. As of the date of reporting the breach, 38 employees/ex-employees had either returned the information (or are in the process of returning) the information to the Organization or the individual concerned, and provided the Organization with a signed acknowledgement form. • Advised unauthorized recipients that the Organization will investigate any reports of the misuse of personal information. Misuse will result in discipline, up to and including loss of employment. • Offered credit monitoring for one year to each affected individual and provided information about how to reduce the risks associated with the breach. • Reviewed and revised processes to ensure the incident does not reoccur.
Steps taken to notify individuals of the incident	Affected individuals were notified of the incident on March 8, 2018 by letter. Supervisors also discussed the breach with affected individuals. Union representatives were also informed.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>Harm 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 the incident could cause “Damage to relationship between [the Organization] and its employees/ex-employees and between employees”. Further, “There is a potential for significant harm because the personal information available on the T4 could be used to commit identity theft or fraud.”</p> <p>I agree with the Organization. The identity and financial information at issue could be used to cause the significant harms of identity theft and fraud, as well as hurt, humiliation and embarrassment.</p>

Real Risk
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 that it believes:

...it is unlikely that harm will result for the following reasons:

- Employees/ex-employees in receipt of the sensitive information have been asked to return the paper records and acknowledge that they have not made or retained any copies, and have not used and will not use the information. As of the date of filing, 38 employees/ex-employees have either returned (or are in the process of returning) the information to the organization or the individual concerned, and provided the company with a signed acknowledgement form. ...*
- Employees/ex-employees have been told that we will investigate any reports that personal information has been misused. [The Organization] is aware which employees/ex-employees received information about another employee/ex-employee, and further, is aware of the specifics of whose information each employee/ex-employee received. The employees have been advised that if they misuse the personal information of another employee/ex-employee they will be subject to discipline, up to and including loss of employment.*
- All affected employees/ex-employees have been provided with notice about the incident and [the Organization] has offered credit monitoring for one year to each affected employee/ex-employee. In addition, each affected employee/ex-employee has been provided with information about how to reduce the risks associated with the breach...*

In my view, there is a real risk of significant harm resulting from this incident, despite the fact the incident did not result from malicious intent (but rather a distribution error), and the Organization's efforts to mitigate risk. At the time of reporting this incident, the Organization had not recovered all the T4 slips, despite the incident occurring over a month prior. In addition, there may be personal/professional relationships between the affected individuals and the unintended recipients, increasing the likelihood of hurt, humiliation or embarrassment, despite the Organization's effort to mitigate harm.

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 distribution error), and the Organization's efforts to mitigate risk.

The identity and financial information at issue could be used to cause the significant harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. At the time of reporting this incident, the Organization had not recovered all the T4 slips, despite the incident occurring over a month prior. In addition, there may be personal/professional relationships between the affected individuals and the unintended recipients, increasing the likelihood of hurt, humiliation or embarrassment, despite the Organization's effort to mitigate harm.

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 affected individuals were notified of the incident on March 8, 2018 by letter. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner