



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Distinct Infrastructure Group Inc., payroll services provider to Pillar Contracting Ltd. (Organization)
Decision number (file number)	P2017-ND-67 (File #005359)
Date notice received by OIPC	April 10, 2017
Date Organization last provided information	May 3, 2017
Date of decision	May 26, 2017
Summary of decision	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).
JURISDICTION	
Section 56 of PIPA “non-profit organization”	The Organization is incorporated in Alberta and 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,• address,• department and position,• employee ID,• pay period start and end dates, and pay date,• amount of remuneration (current and year to date). <p>The information above is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure	

<p>Description of incident</p>	<ul style="list-style-type: none"> • The Organization provides payroll services to its subsidiary company, Pillar Contracting Ltd. • On October 27, 2016, the Organization inadvertently emailed pay stubs of 17 employees of the subsidiary company to two current employees and two former employees. • On the same day, one of the individuals who received the email notified a Supervisor with the subsidiary company of the incident. The subsidiary advised the Organization of the incident on October 28, 2016. • The Organization asked the individual who notified the subsidiary he received the email to delete it and contacted the other recipients of the email to request they delete the email without opening it. The Organization reported that all of the other recipients agreed to do so; however there is some evidence that at least one of the unauthorized recipients opened the attachments. • The Organization determined that the cause of the breach was human error.
<p>Affected individuals</p>	<p>The incident affected 17 individuals who are residents of Alberta.</p>
<p>Steps taken to reduce risk of harm to individuals</p>	<p>The Organization addressed the incident with the payroll administrator and outsourced its payroll functions to another provider.</p>
<p>Steps taken to notify individuals of the incident</p>	<p>The Organization has not taken any steps to notify affected individuals.</p>
<p>REAL RISK OF SIGNIFICANT HARM ANALYSIS</p>	
<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>In its report of the breach, the Organization stated “The information disclosed to the employees did not contain any information that posed a risk of significant harm to the employees whose information was disclosed. The only harm to the employees whose information was disclosed is one of embarrassment with respect to their earnings.”</p> <p>In my view, and consistent with previous breach decisions issued by my office (e.g. P2015-ND-29), the employment information at issue could be used to cause the significant harms of hurt, humiliation and embarrassment.</p>

<p>Real Risk</p> <p>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 “There is a very low likelihood that any significant harm could result due to the disclosure of the personal information.”</p> <p>In my view, there is a real risk of harm resulting from this incident. Although the breach was not the result of malicious intent, there is some evidence that at least two of the individuals who received the emails opened the attachments containing the personal information and are aware of the contents. The professional relationship between the affected individuals and the unauthorized recipients of the information increases the risk of hurt, humiliation or embarrassment resulting in this case.</p>
<p>DECISION UNDER SECTION 37.1(1) OF PIPA</p>	
<p>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 employment information at issue could be used to cause the significant harms of hurt, humiliation and embarrassment. Although the breach was not the result of malicious intent, there is some evidence that at least two of the individuals who received the emails opened the attachments containing the personal information and are aware of the contents. The professional relationship between the affected individuals and the unauthorized recipients of the information increases the risk of hurt, humiliation or embarrassment resulting in this case.</p> <p>I require the Organization to notify affected individuals in Alberta in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> and provide me with written confirmation that it has done so on or before June 9, 2017.</p>	

Jill Clayton
Information and Privacy Commissioner