



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

<b>Organization providing notice under section 34.1 of PIPA</b>	Wayside Technology Group, Inc. (Organization)
<b>Decision number (file number)</b>	P2020-ND-126 (File# 013868)
<b>Date notice received by OIPC</b>	November 15, 2019
<b>Date Organization last provided information</b>	November 15, 2019
<b>Date of decision</b>	October 27, 2020
<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 individual whose personal information was collected in Alberta 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 incident involved all or some of the following information:</p> <ul style="list-style-type: none"><li>• driver's license/identification card number,</li><li>• medical/health information and health insurance number,</li><li>• financial account information,</li><li>• tax identification number, and</li><li>• date of birth.</li></ul> <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.</p>
<b>DESCRIPTION OF INCIDENT</b>	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
<b>Description of incident</b>	<ul style="list-style-type: none"><li>• On June 20, 2019, the Organization discovered unusual activity involving its email system which occurred between June 12 and June 13, 2019.</li></ul>

	<ul style="list-style-type: none"> <li>On October 9, 2019, the Organization’s investigation revealed that personal information may have been accessed without authorization.</li> </ul>
<b>Affected individuals</b>	A total of 1,228 individuals were affected, including 1 Alberta resident.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>Terminated unauthorized access, investigated and engaged a digital forensics firm to determine what happened, whether personal information was accessed, and to identify the scope of data subjects affected.</li> <li>Implemented a number of additional security features to minimize the likelihood of a similar incident in the future.</li> <li>Offered affected individuals complimentary fraud consultation and identity theft restoration services.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	Affected individuals were notified by letter on November 15, 2019.
<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 it “...is not in possession of evidence as to whether the unauthorized actor did, in fact, access or exfiltrate any personal information as a result of the incident. However, out of an abundance of caution [the Organization] notified the one (1) resident of Alberta whose information may have been affected in order to advise the individual of the incident and offer complimentary Fraud Consultation and Identity Theft Restoration services [sic] ... as a further proactive measure to mitigate any risk of harm.”</p> <p>In my view, a reasonable person would consider the identity, financial and tax information at issue could be used to cause the harms of identity theft and fraud. Health information could be used to cause the harms of hurt, humiliation and embarrassment. These are all significant harms.</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 it “... is not in possession of evidence as to whether the unauthorized actor did, in fact, access or exfiltrate any personal information as a result of the incident.”</p> <p>In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to malicious action. The Organization cannot rule out the possibility that the unauthorized party accessed or exfiltrated the personal information at issue.</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.

A reasonable person would consider the identity, financial and tax information at issue could be used to cause the harms of identity theft and fraud. Health information could be used to cause the harms of hurt, humiliation and embarrassment. These are all significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to malicious action. The Organization cannot rule out the possibility that the unauthorized party accessed or exfiltrated the personal information at issue.

I require the Organization to notify the affected individual whose personal information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation*. I understand the Organization notified the affected individuals by letter on November 15, 2019. The Organization is not required to notify the affected individual again.

Jill Clayton  
Information and Privacy Commissioner