



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	TALX Corporation and Allegis Group Inc. (the Organizations), as reported by TALX Corporation
Decision number (file number)	P2019-ND-030 (File #005694)
Date notice received by OIPC	May 23, 2017
Date Organization last provided information	November 3, 2017
Date of decision	February 19, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organizations are required to notify the individuals in Alberta, pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	The Organizations are both “organizations” as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	<p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none">• name,• address,• email address,• date of birth,• Social Insurance Number,• wage and direct deposit information• employee identification number,• gender,• marital status, and• any information on W-2, 1095-C, T4 and RL-1 tax forms. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. Some of the information concerns three Alberta employees of Allegis.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	

<p>Description of incident</p>	<ul style="list-style-type: none"> • TALX Corporation provides certain payroll related services to Allegis, which allows Allegis’ employees to access electronic copies of tax forms through an online portal website. • On February 1, 2017, TALX Corporation discovered that an Allegis employee reported an unauthorized change to the email address associated with the employee’s online portal account. • The Organizations investigated and determined that the unauthorized person(s) was able to successfully answer questions about the affected individuals in order to reset the individuals’ PINs. There is no indication that either of the Organizations were the source of any of the information used to reset the PINs and access the accounts. • It appears that unauthorized access occurred between January 4, 2016 and March 29, 2017.
<p>Affected individuals</p>	<p>The incident affected 40,645 individuals, including three (3) Alberta residents.</p>
<p>Steps taken to reduce risk of harm to individuals</p>	<ul style="list-style-type: none"> • An investigation was launched and an independent cybersecurity firm was retained to assist in the investigation and identifying affected individuals. • Implementing additional security measures to help prevent recurrence of this type of incident. • Offered affected individuals twenty-four (24) months of credit file monitoring.
<p>Steps taken to notify individuals of the incident</p>	<p>The affected individuals in Alberta were notified by letter on May 17, 2017.</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>The Organizations reported “The individuals affected by this incident may be at risk of identity theft. Additionally, because tax forms may have been accessed without authorization, it is possible that a third party could attempt to file a fraudulent tax return.”</p> <p>I agree with the Organizations. The financial and identity information at issue could be used to cause the harms of fraud, identity theft and financial loss. These are significant harms.</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 Organizations reported that “TALX is unable to definitively state whether any particular individual will suffer negative consequences from the incident. However, [the] investigation indicates that some of the unauthorized accesses may have been carried out to facilitate tax return fraud.”</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the information may have been exposed for approximately fifteen (15) months.</p>
<p>DECISION UNDER SECTION 37.1(1) OF PIPA</p>	
<p>Based on the information provided by the Organizations and given the circumstances of the incident, I have decided that there is a real risk of significant harm resulting from this incident.</p> <p>The financial and identity information at issue could be used to cause the harms or fraud, identity theft and financial loss. These are significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the information may have been exposed for approximately fifteen (15) months.</p> <p>I require the Organizations to notify the affected individuals in Alberta in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the Organizations notified the affected individuals by letter on May 17, 2017, in accordance with the Regulation. The Organizations are not required to notify the affected individuals again.</p>	

Jill Clayton
Information and Privacy Commissioner