Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	TALX Corporation and Honeywell International Inc. (the Organizations), as reported by TALX Corporation
Decision number (file number)	P2019-ND-044 (File #005490)
Date notice received by OIPC	May 9, 2017
Date Organization last provided information	November 11, 2017
Date of decision	March 4, 2019
Summary of decision	There is a real risk of significant harm to the individual in Alberta affected by this incident. The Organizations are required to notify the individual pursuant to section 37.1 of the *Personal Information Protection Act* (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"	The incident involved all or some of the following information: • name, • address, • email address, • telephone number, • date of birth, • Social Insurance Number, • employee identification number, • gender, • marital status, and • information included on T4 and RL-1 tax forms. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• TALX Corporation provides certain payroll related services to Honeywell International Inc. which allows Honeywell's employees to access electronic copies of T4 and RL-1 tax forms through an online portal website. • On February 8, 2017, TALX Corporation discovered that one or more persons reset the PINs and accessed the online portal accounts of a small number of current and former Honeywell employees. The resets were unauthorized, and the unauthorized person(s) may have accessed any of the information maintained in the online portal. • TALX Corporation's investigation 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 July 2016 and March 2017.
Affected individuals	The incident affected 33 individuals, including 1 Alberta resident.
Steps taken to reduce risk of harm to individuals	• 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 twelve (12) months of credit file monitoring.
Steps taken to notify individuals of the incident	The affected individual in Alberta was notified by letter on April 28, 2017.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
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.	The Organizations reported "The individuals affected by this incident may be at risk of having their identity stolen. 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 in an employee's name." I agree with the Organizations. 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.

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 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 identify theft and/or tax return fraud." 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 nine (9) months.

DECISION UNDER SECTION 37.1(1) OF PIPA

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 to the affected individual in Alberta.

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 nine (9) months.

I require the Organizations to notify the affected individual in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organizations notified the affected individual in letter dated April 28, 2017, in accordance with the Regulation. The Organizations are not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner