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	Trailer Wizards Ltd. (Organization)
Decision number (file number)	P2017-ND-77 (File#005040)
Date notice received by OIPC	February 21, 2017
Date Organization last provided information	March 27, 2017
Date of decision	June 12, 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 those individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is federally incorporated and operating in Alberta. It is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • electronic copies of direct deposit forms containing banking information, • electronic copies of employee information forms including telephone numbers and addresses, • electronic copies of doctor's notes indicating employees' ability to return to work from medical leaves and indicating employees with mental illnesses, • electronic copies of disciplinary letters, • driver's license numbers and electronic copies of driver's licenses, • electronic copies of resumes, • salary and title information, • benefits Information, and • job training records. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from employees of the Organization across Canada.

DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On February 8, 2017, an employee with the Organization discovered that she had access to employee files she did not normally have access to and reported it to the Organization. • The Organization investigated and found that permission settings on shared file drives were lost during migration of data to a new server. • The Organization reported it is possible unauthorized access began in January 2015 when the server was provisioned and data migrations began. The information was accessible to internal employees who had a valid account between the period of January 2015 and February 9, 2017; however, many employees were not able to view the folders as they were not mapped on their network drive. • The Organization is unable to confirm whether or not the files were actually accessed as detailed access logging and auditing was not enabled. • The breach affected the Organization's entire workforce of current and past employees.
Affected individuals	The incident affected 450 individuals, of which 85 are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Locked file servers to all employees while permission settings were restored and corrected permission settings. • Communicated to all affected employees regarding the breach. • Reviewed the security access control list, disabled inherited permissions, enabled file access logging, identified and implemented an Access Auditing solution, ensured administration of sensitive folders will be performed by IT Managers only, and implemented a periodic review schedule to ensure access reflects employee roles.
Steps taken to notify individuals of the incident	Affected individuals were notified in person, by email and letters sent February 10, 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 Organization reported the possible harm that might result from this incident included "Financial loss, fraud or identity theft due to the sensitivity of the personal information. Humiliation or damage to reputation due to the nature of disciplinary and medical information contained in the files." I agree with the Organization. The comprehensive contact, identity, employment and health information at issue could be used to cause the harms of identity theft, fraud, financial loss, hurt, humiliation, embarrassment and damage to reputation. 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 Organization reported that "It is unknown whether any employees attempted to access these confidential folders" and also that "While the information could have only been obtained by internal employees (not external), the information contained was highly sensitive and could be used for criminal purposes. However, we do not know of any employees who were aware of this breach (other than those in positions of trust). We are unsure of how long the information was exposed at this time. There is no evidence of malicious intent at this time." In my view, there is a real risk of harm in this case. Although the incident resulted from a system error and not malicious intent, the Organization does not know whether personal information was actually accessed as detailed access logging and auditing was not enabled. The Organization later reported it is possible the information was exposed for 2 years. The likelihood of hurt, humiliation and embarrassment is increased due to the personal and professional relationships between the affected individuals and employees who may have had unauthorized access to the information.
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. The comprehensive contact, identity, employment and health information at issue could be used to cause the harms of identity theft, fraud, financial loss, hurt, humiliation, embarrassment and damage to reputation. These are significant harms. Although the incident resulted from a system error and not malicious intent, the Organization does not know whether personal information was actually accessed as detailed access logging and auditing was not enabled. The Organization later reported it is possible the information was exposed for 2 years. The likelihood of hurt, humiliation and embarrassment is increased due to the personal and professional relationships between the affected individuals and employees who may have had unauthorized access to the information.	

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

I understand the Organization all affected individuals were notified in person, by email and letters sent February 10, 2017. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner