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	Universal Rail Systems (Organization)
Decision number (file number)	P2018-ND-128 (File #007958)
Date notice received by OIPC	March 2, 2018
Date Organization last provided information	September 17, 2018
Date of decision	September 27, 2018
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 provincially regulated and is an "organization" 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, • social insurance number, • address, • yearly earnings and deductions, and • employer RN number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• During a routine payroll systems upgrade, a new system folder provided by a third party vendor was installed by the Organization's IT department. The system generates automatic emails to employees with their T4s.

	• The Organization tested the system before releasing T4s. However, after releasing the first department's T4s, the payroll department reviewed a sampling of emails and discovered that each employee received only one T4 statement instead of two duplicates, and every second employee received a copy of the previous employee's T4 statement. • The emails sent in error were in employee inboxes for approximately 30 minutes. Employees were instructed to immediately and permanently delete the previous T4 emails. • The Organization discovered that that the folder with the new tax table installed had back-end system coding that changed options for payroll to select when releasing the T4s. • The incident occurred on February 2, 2018 and was discovered the same day.
Affected individuals	The incident affected 22 individuals.
Steps taken to reduce risk of harm to individuals	• Emailed and personally called all employees impacted by the breach. • Instructed employees to immediately and permanently delete the unintended email. • Amended procedures to provide for more detailed testing of any system upgrade. • No longer copying and pasting system folders to ensure back-end system coding is not impacted. • Amended processes to ensure that all views are reviewed prior to T4 statements being released. • Researching other systems that allow statement "recall" as a fail-safe in the event of system errors. • Offered all impacted employees a 12 month subscription to Equifax to mitigate any potential financial harm.
Steps taken to notify individuals of the incident	Affected individuals were notified verbally and by email on February 13, 2018.
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 that "As the information included financial information, name, address and SIN number there is a risk of potential fraud and identity theft." I agree with the Organization. The contact, identity and financial information at issue could be used to cause the significant harms of identity theft and fraud. Further, because the information was mistakenly provided to employees in the same department, the employment information (earnings) could be used to cause the significant harms of hurt, humiliation and embarrassment.

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 "The likelihood of harm is relatively small. The T4s were sent to a single department, not company wide, and all individuals were contacted immediately and informed of the breaches. All employees are required to sign employment agreements that contain clauses regarding confidentiality, privacy, and appropriate conduct. All employees are expected to adhere to the confidentiality and privacy provisions of the employment agreements. Given that all employees who accidentally received an incorrect T4, and all employees who had their T4 disclosed, were notified about the disclosure, it would be unlikely any employee would use that information for criminal purposes". The Organization also reported that "…the emails had been in their inboxes for approximately 30 minutes until they were notified of the error… All employees were instructed to immediately and permanently delete the previous T4 emails containing the information". I agree with the Organization that it is unlikely the information at issue will be used to cause the significant harms of identity theft and/or fraud. The Organization knows which employees received the T4s in error and instructed that the emails containing the T4s be permanently deleted. However, although the incident was the result of human error and not malicious intent, and the Organization acted quickly to report the matter to the affected individuals, there is a personal/professional relationship between the unauthorized recipients and the affected individuals, which increases the likelihood that embarrassment, hurt, humiliation and embarrassment could result.

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 contact, identity and financial information at issue could be used to cause the significant harms of identity theft and fraud. Further, because the information was mistakenly provided to employees in the same department, the employment information (earnings) could be used to cause the significant harms of hurt, humiliation and embarrassment.

It is unlikely the information at issue will be used to cause the significant harms of identity theft and/or fraud. The Organization knows which employees received the T4s in error and instructed that the emails containing the T4s be permanently deleted.

However, although the incident was the result of human error and not malicious intent, and the Organization acted quickly to report the matter to the affected individuals, there is a personal/professional relationship between the unauthorized recipients and the affected individuals, which increases the likelihood that embarrassment, hurt, humiliation and embarrassment could result.

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 notified affected individuals verbally and in an email dated February 13, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner