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	Railworks Corporation (Organization)
Decision number (file number)	P2020-ND-097 (File #015229)
Date notice received by OIPC	February 27, 2020
Date Organization last provided information	February 27, 2020
Date of decision	September 3, 2020
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individuals whose personal information was collected in Alberta, pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization's head office is in New York, NY, USA. The Organization 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, • address, • Social Security number, • driver's license number and/or government issued ID, • dates of birth, and/or • dates of hire/termination and/or retirement, as applicable. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On January 27, 2020, the Organization was the victim of a cyberattack in which an unauthorized third party encrypted its systems and files that contained personal information of its employees, former employees, current and former employees' beneficiaries / dependents and some independent contractors. • The incident ended on January 31, 2020.
Affected individuals	The incident affected 23,751, including 427 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Offered affected individuals free credit monitoring services for twelve (12) months. • Engaged a cyber security firm to assist with the investigation and remediation efforts. • Conducted an investigation and strengthening IT infrastructure.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on February 27, 2020.
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 it "…does not have any indication of misuse of the information, but out of an abundance of caution and to help protect the affected individuals' financial security, [the Organization has] notified all affected individuals". In my view, a reasonable person would consider the contact (name and address) and identity information (Social Security numbers, driver's license number and date of birth) at issue could be used to cause the significant harms of identity theft, and fraud.
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 "No indication of misuse of information, but due to the sensitive nature of the information involved (i.e. Social Security numbers), [the Organization] notified individuals under PIPA". 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, unauthorized encryption of files). The information was compromised for approximately 5 days. The fact that there is "no indication of misuse" of the information does not mitigate against the possibility of future use of the information to cause the harms of identity theft and/or fraud.

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 contact (name and address) and identity information (Social Security numbers, driver's license number and date of birth) at issue could be used to cause the significant harms of identity theft, and fraud. 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, unauthorized encryption of files). The information was compromised for approximately 5 days. The fact that there is "no indication of misuse" of the information does not mitigate against the possibility of future use of the information to cause the harms of identity theft and/or fraud. I require the Organization to notify the affected individuals whose personal information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals by letter on February 27, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner