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	Steele's Transfer Ltd. and Steele's Total Logistics Ltd. o/s Steele's Transportation Group (collectively, the "Organization")
Decision number (file number)	P2019-ND-049 (File #011508)
Date notice received by OIPC	January 6, 2019
Date Organization last provided information	January 6, 2019
Date of decision	May 1, 2019
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 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 is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • address, • email address, • telephone and cell number, • employment start and end date, • insurance company and policy number, and • driver's license number and expiry date. 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	• On November 18, 2018, the Organization discovered that it was the victim of a ransomware attack. • The Organization retained third party computer forensic experts to investigate and assist with decryption. The investigation found that the threat actor's activities were limited to encrypting files and that there was no evidence that any files were accessed, viewed or exfiltrated, with one exception: the threat actors clicked on an existing shortcut on November 18, 2018, which linked to a server that contained the personal information at issue for 68 drivers that worked for the Organization. The Organization cannot determine whether this information was accessed, viewed or exfiltrated. • The breach was confirmed to be contained on November 20, 2018.
Affected individuals	The incident affected 68 individuals.
Steps taken to reduce risk of harm to individuals	• Shut down all computers. • Decrypted and restored the files. • Reviewed firewall traffic for atypical activities and found normal traffic. • Disabled all outbound traffic and incoming firewall traffic to prevent re-entry. • Closed the remote desktop protocols to prevent re-entry. • Changed all relevant passwords. • Reported breach to law enforcement. • Offered affected individuals free credit monitoring for one year. • Notified clients and other staff of the incident. • Will provide office staff with training regarding additional security awareness training through a third party provider.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on November 22 and 23, 2018. A second notification letter will be emailed to provide additional information.
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 harms could include fraud, or phishing campaigns where the threat actors could infect the emails or computers of the drivers". I agree with the Organization's assessment. In my view, a reasonable person would consider that the contact, employment, insurance and identity information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, resulting in an increased vulnerability to identity theft and fraud. 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 "There is a reasonable likelihood that harm could result because this was an intentional and malicious ransomware attack perpetrated by hackers who are looking to profit from the attack". In my view, a reasonable person would consider that 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 and ransomware).

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 that the contact, employment, insurance and identity information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, resulting in an increased vulnerability to identity theft and fraud. 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 and ransomware).

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 affected individuals were notified by email on November 22 and 23, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner