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	Canpar Express Inc. (Organization)
Decision number (file number)	P2021-ND-339 (File #017873)
Date notice received by OIPC	October 26, 2020
Date Organization last provided information	October 26, 2021
Date of decision	March 10, 2022
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 operates in Alberta 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, • address, • salary, • Social Insurance Number, • credit card number including CVV, and • signature. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent that the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On August 19, 2020, the Organization discovered that it was victim to ransomware.

	• The attack began on or about August 13, 2020 when a server was infected with malware. Several strains of malware, use of offensive tools (Cobalt Strike), and lateral movement of the attacker(s) to other systems were reported. • On September 14, 2020, the Organization discovered that exfiltrated records were leaked on the Dark Web. • It is not known how the attackers initially compromised the Organization's network.
Affected individuals	The incident affected 6,715 individuals, including 1,100 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately shut-down servers and endpoints. • Disabled public facing websites and portals. • Retained the services of a cyber-risk management company and investigated the incident. • Offered credit monitoring services to affected individuals. • Implemented multi-factor authentication, end-point detection and response, and education programs. • Implemented testing of prevention plans and made amendments to cybersecurity policies.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter. Letters were dated October 7, 2020 and mailed on October 16, 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 "The potential risks we have identified were of possible use of information of financial nature: unauthorized use of credit cards; fraud or identity theft using SIN numbers and other related personal information." I agree with the Organization's assessment. A reasonable person would consider that the financial and identity information at issue could be used to cause the significant harms of fraud, identity theft, financial loss, and negative effects on a credit record.
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 did not provide an assessment of the likelihood that significant harm will result. 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 a third party (deliberate intrusion, deployment of malware, exfiltration and publication of records). Further, the threat actor had access to the Organization's network for 6 days prior to the discovery of the breach.

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 financial and identity information at issue could be used to cause the significant harms of fraud, identity theft, financial loss, and negative effects on a credit record. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (deliberate intrusion, deployment of malware, exfiltration and publication of records). Further, the threat actor had access to the Organization's network for 6 days prior to the discovery of the breach. 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 October 16, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner