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	Backroads Canada Corporation (Organization)
Decision number (file number)	P2021-ND-301 (File #020331)
Date notice received by OIPC	March 25, 2021
Date Organization last provided information	March 25, 2021
Date of decision	March 3, 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 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: • first and last name, • date of birth, • email address, • residential address, • social insurance number, • photocopy of passport or photocopy of driver licence for some of the affected individuals, • financial account information, and • health insurance information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On October 2, 2020, the Organization's parent company discovered certain portions of its network and workstations were impacted by a ransomware incident. • On October 9, 2020, a forensic investigation discovered that human resources data was potentially exfiltrated. • On or around October 16, 2020, it was confirmed that Canadian employee information was part of the exfiltrated data. • The breach was discovered on October 16 through the use of early detection and response software, which detected abnormal behaviour and was able to stop the encryption of the majority of the data. • The Organization reported the breach occurred between October 2, 2020 and October 5, 2020.
Affected individuals	The incident affected 435 Canadians, including 146 in Alberta.
Steps taken to reduce risk of harm to individuals	• Notified data protection authorities, as well as law enforcement. • Introduced multifactor authentication and other information security measures. • In the process of: o implementing a Security Information and Event Management (SIEM), to aggregate and analyze activity from different resources across the IT infrastructure. o working with vendors to protect guest/employee data. o identifying an HRIS system to protect employee information, and ensure compliance in multiple locations. • Offered one-year credit monitoring to affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by email in December 17, 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 possible consequences might include identity theft, fraud, loss of confidentiality of personal data and phishing." In my view, a reasonable person would consider the contact, identity, insurance and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. Health insurance information could also be used to cause embarrassment and humiliation. 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… *…considers that the likelihood that harm will result is low given that the threat actors' incentive was to encrypt the systems in order to obtain a ransom payment.* 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, ransom demand). The information was exposed for 3 days. Although the Organization reported that "the threat actors' incentive was to encrypt the systems in order to obtain a ransom payment", I do not find this to be reassuring. The Organization can only speculate as to the motives of the thief.

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, identity, insurance and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. Health insurance information could also be used to cause embarrassment and humiliation. 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, ransom demand). The information was exposed for 3 days. Although the Organization reported that "the threat actors' incentive was to encrypt the systems in order to obtain a ransom payment", I do not find this to be reassuring. The Organization can only speculate as to the motives of the thief.

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 email on December 17, 2021. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner