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	Rowland, Parker & Associates LLP (Organization)
Decision number (file number)	P2021-ND-342 (File #020867)
Date notice received by OIPC	May 6, 2021
Date Organization last provided information	August 24, 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, • date of birth, and • social insurance number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On April 2, 2021, the Organization found it was unable to log into workplace servers. The Organization engaged its IT service provider who determined that threat actors accessed the network and client personal information without authorization.

	• Shortly after discovery, the threat actors contacted the Organization and confirmed the breach. • Based on the Organization's investigation, it is believed that a phishing campaign lead to the attack involving ransomware. • It is also reported that the threat actors destroyed copies of the personal information obtained in the attack.
Affected individuals	The incident affected 1,570 individuals.
Steps taken to reduce risk of harm to individuals	• Blocked the unauthorized access. • Engaged cyber security experts to contain and investigate the incident. • Received confirmation that copies of exfiltrated personal information were destroyed by the threat actor. • Offered affected individuals a year of credit monitoring services. • Immediately implemented 2-step authentication for all servers and programs. • Engaged external IT to conduct regular security assessments. • Continuing to investigate further areas to harden.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on May 4, 2021.
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: "It is possible that individual's information may be used to fraudulently steal their identity." I agree with the Organization's assessment. A reasonable person would consider the identity (date of birth, social insurance number) information at issue could be used to cause the significant harms of identity theft or 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 that it… *… believes that the likelihood of harm is low. The threat actor was cooperative in the process, and provided proof that they destroyed their copy of the personal information obtained. [The Organization] does not have reason to believe there are additional copies of the stolen information.* In my view, a reasonable person would consider 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, exfiltration of data, deployment of ransomware). Although the threat actor "provided proof that they destroyed their copy of the personal information", the possibility that other copies exist cannot be ruled out despite the Organization's belief otherwise.

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 identity (date of birth, social insurance number) information at issue could be used to cause the significant harms of identity theft or fraud.

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, exfiltration of data, deployment of ransomware). Although the threat actor "provided proof that they destroyed their copy of the personal information", the possibility that other copies exist cannot be ruled out despite the Organization's belief otherwise.

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 May 4, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner