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	Rocky Mountain House Society dba Rocky Mountain Support Services Society (Organization)
Decision number (file number)	P2021-ND-064 (File #013317)
Date notice received by OIPC	May 24, 2019
Date Organization last provided information	December 19, 2019
Date of decision	March 9, 2021
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	The Organization reported that it is incorporated under Alberta’s *Societies Act* and therefore is a “non-profit organization” as defined in section 56(1)(b)(i) of PIPA. Pursuant to section 56(2), PIPA “does not apply to a non-profit organization or any personal information that is in the custody of or under the control of a non-profit organization”, except in the case of personal information that is collected, used or disclosed in connection with any commercial activity. To the extent the personal information at issue was collected in connection with any commercial activities of the Organization, PIPA applies.
Section 1(1)(k) of PIPA “personal information”	The incident involved all or some of the following information: • full name, • address, • telephone number, • bank account number, • social insurance number, and • date of birth.

	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 May 19, 2019, the Organization experienced a ransomware attack that encrypted the Organization’s systems. • The Organization’s IT reported that an email was sent May 14, 2019 which activated a virus. • The breach was discovered on May 21, 2019. • The Organization was able to recover its data and, although it is unaware of any evidence to suggest that its data was accessed or exfiltrated, it was not able to conclusively determine the issue.
Affected individuals	The incident affected approximately 113 clients, staff and past employees.
Steps taken to reduce risk of harm to individuals	• Notified present and past employees. • Secured work stations, servers and back-up servers. • Reset email, login passwords, and VPN passwords • Upgraded to SSL and upgraded Microsoft Office. • Notified the RCMP and the Information and Privacy Commissioner. • Offering one-year of free credit and identity theft monitoring.
Steps taken to notify individuals of the incident	Affected individuals were notified verbally between May 20 and 28, 2019 and provided further written notification letters by mail and email to all affected individuals, including former employees, between October 7 and 17, 2019. There were 7 affected individuals for whom the Organization does not have current or direct contact information. The Organization posted a notice with a link to the notification letter on the front page of its website.
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	The Organization reported that, “where bank account information is involved there is a real risk of significant harm of financial fraud. Other categories of personal information also raise the risk of other categories of fraud, such as identity theft, and the disclosure of contact information raises a risk of phishing.” I agree with the Organization’s assessment. A reasonable person would consider the contact and identity information (date of birth,

non-trivial consequences or effects.	social insurance number) 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 did not specifically assess the likelihood that significant harm would result from this incident but did report that it is “unaware of any information or activity which suggests that its data was accessed or exfiltrated by the attacker; however, (it) has not been able to conclusively determine the issue.” 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 an unknown third party (deliberate intrusion and ransomware). The Organization was able to restore data and functionality from backups; however, the Organization is unable to rule out unauthorized access or exfiltration of the personal information at issue.

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 and identity information (date of birth, social insurance number) 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 and ransomware). The Organization was able to restore data and functionality from backups; however, the Organization is unable to rule out unauthorized access or exfiltration of the personal information at issue.

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 the affected individuals by letter or email between October 7 and 17, 2019 in accordance with the Regulation. The Organization is not required to notify these affected individuals again.

In this case, the Organization reported that it could not notify seven (7) individuals because it did not have current or direct contact information for these individuals. However, the Organization provided substitute notice by way of a notice on its website homepage: (https://www.rockysupportservices.ca/content/4/).

Section 19.1(2) of the Regulation states that “the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances.”

Given the Organization’s submissions, I accept that indirect or substitute notice as described by the Organization is reasonable in this case, where the Organization is unable to contact affected individuals directly.

Jill Clayton
Information and Privacy Commissioner