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	USNR, LLC (Organization)
Decision number (file number)	P2021-ND-200 (File #018549)
Date notice received by OIPC	December 4, 2020
Date Organization last provided information	August 3, 2021
Date of decision	October 18, 2021
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 headquartered in Woodland, Washington, USA, 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 about current and former employees: • name, • postal address, • date of birth, • social insurance number, and • bank account information. The name, postal address, date of birth, and social insurance number of beneficiaries were also affected. 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 or about September 28, 2020, an employee downloaded and executed a malicious software (Chrome) update. The malicious update contained malware that enabled attackers to remotely access the Organization's network without authorization. • On October 25, 2020, approximately a month after the initial breach, the attackers encrypted various systems. The intrusion was detected on the same day when encrypted files and a ransom note were found. • It is reported that the attacker was able to access the personal information of current and former employees stored on the Organization's information systems during the attack.
Affected individuals	The incident affected 1,234 individuals in Canada, including 2 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately took all servers and systems offline and sanitized infected devices. • Rebuilt systems that could not be sanitized. • Worked with a cybersecurity firm to rebuild network and infrastructure. • Engaged in a detailed review of cybersecurity policies and procedures. • Conducted a forensic examination of the Organization's network. • Offered affected individuals 12 months of identity monitoring services.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on December 7, 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: *Based on the nature of the incident, the possible harms that might occur as a result of the breach could include fraud/phishing emails and identity theft.* I accept the Organization's assessment. A reasonable person would consider that the contact, identity, and financial information (including the personal information of beneficiaries) 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 reported it... *... is not aware of any actual or attempted access or misuse of the personal information of its employees and former employees and their beneficiaries and has no indication that any harm has occurred as a result of the incident. In light of the foregoing, [the Organizaiton] is of the view that the breach does not present any real risk of significant harm to any individual.* Additionally, the Organization reported: *…the primary intent of the attack looks to have been to disrupt... operations … [and] that we have no evidence of such information being viewed, stolen, or otherwise misused…* 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 a third party (deliberate intrusion and ransom demand). The Organization did not rule out the possibility that the personal information was exfiltrated. Further, a lack of evidence of misuse of personal information to date does not mitigate against future harm since identity theft and fraud can occur months or years after a breach. Additionally, the attackers were able to access the Organization's network for approximately one month before the intrusion was detected and contained.

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, identity, and financial information (including the personal information of beneficiaries) 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 a third party (deliberate intrusion and ransom demand).

The Organization did not rule out the possibility that the personal information was exfiltrated. Further, a lack of evidence of misuse of personal information to date does not mitigate against future harm since identity theft and fraud can occur months or years after a breach.

Additionally, the attackers were able to access the Organization's network for approximately one month before the intrusion was detected and contained.

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 December 7, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner