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	Anvil Corporation (Organization)
Decision number (file number)	P2021-ND-222 (File #020858)
Date notice received by OIPC	April 30, 2021
Date Organization last provided information	September 3, 2021
Date of decision	November 12, 2021
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual 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 Bellingham, WA, USA, and is an "organization" as defined in section 1(1)(i) of PIPA. The Organization does not operate in Alberta, however, the affected individual is an employee who resides in the province.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, and • social security number. This information is about an identifiable individual 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 March 11, 2021, the Organization suffered a ransomware attack. It was later determined that the attacker had access to the Organization's network as early as February 9, 2021. The root cause of the initial breach was not reported. • On April 12, 2021, the Organization's investigation determined that attackers were able to view and download records containing the personal information of current and former employees.
Affected individuals	The incident affected 1 resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Notified the Federal Bureau of Investigation (FBI). • Implemented continuous threat monitoring. • Reconfigured firewalls to permit only specified network traffic. • Implemented multi-factor authentication. • Decommissioned and retired end-of-life hardware and software. • Provided individuals with guidance on detecting fraud and offered credit monitoring services.
Steps taken to notify individuals of the incident	The affected individual in Alberta was notified by letter on April 30, 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 the possible harms of "identity theft or financial fraud." I agree with the Organization's assessment. A reasonable person would consider the identity information at issue (name and social security number) 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 that it... *... is not aware of any fraud or identity theft to any individual as a result of this incident and cannot confirm if any personal information was actually viewed or downloaded by the unauthorized party. Nevertheless, [the Organization] is notifying all individuals whose personal information could have been viewed and downloaded. [The Organization] is also offering all of these individuals complimentary credit monitoring.* *In [the Organization's] determination, the likelihood that harm will result from this Incident is low. To date, [the*

	Organization] has received no reports of fraud related to the Incident, and ... has no reason to believe that the unauthorized party made the information believed to be involved public or otherwise used it. Moreover, [the Organization] has provided involved parties with complimentary identify theft protection services designed to prevent attempted fraud. 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, ransomware). The lack of reported fraud or identity theft does not mitigate against future harm as such harms can occur months or years after a breach. Further, the threat actor had access to the Organization's network for approximately one month before the breach was ended.

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 individual.

A reasonable person would consider the identity information at issue (name and social security number) 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, ransomware). The lack of reported fraud or identity theft does not mitigate against future harm as such harms can occur months or years after a breach. Further, the threat actor had access to the Organization's network for approximately one month before the breach was ended.

I require the Organization to notify the affected individual 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 individual by letter on April 30, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner