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	Worth Ventures Ltd. (Organization)
Decision number (file number)	P2021-ND-035 (File #016227)
Date notice received by OIPC	June 12, 2020
Date Organization last provided information	June 12, 2020
Date of decision	February 23, 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 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 Organization reported: *The type of personal information has been withheld from [us], but given that we have payroll systems on one of the PCs that was attacked, it seems reasonable to assume that; name, social insurance number, birthdates, healthcare numbers, home address, bank account numbers and payroll records would be compromised.* This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization participates in a joint venture with another organization, MegaSys Enterprises Ltd. (MegaSys), that is responsible for the integrity of the computer network.

	• On May 11, 2020, ransomware encryption was triggered and the perpetrator indicated that personal files have been downloaded although the Organization cannot confirm this. All of the Organization's Windows based PCs connected to the domain server were attacked by the ransomware. • The breach was discovered initially by an external customer who was attempting to connect to the Organization's software ticketing system. • The Organization reported that MegaSys "has refused to provide much information … about this breach".
Affected individuals	The incident affected approximately 200 Alberta residents.
Steps taken to reduce risk of harm to individuals	The Organization reported that "…information has been provided to allow existing staff to contact; Canadian Anti-Fraud Centre, Canada Post, Equifax Canada, TransUnion Canada, Service Canada."
Steps taken to notify individuals of the incident	Forty-one (41) employees were notified by email on May 14, 2020. The Organization reported that it has "…been advised that information on over 200 individuals existsed [sic], does not know if these additional individuals have been notified (approximately [sic] 160). That information is with MegaSys…".
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, *Possible identity theft is the major one, but potentially unauthorized access to an employee bank account and/or unauthorized access to health information.* In my view, a reasonable person would consider the contact, identity, financial, employment and health information potentially at issue could be used to cause the harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. These are all significant harms. Because the Organization cannot confirm whether other personal information might have been accessed, it is not clear what other possible harms may exist.
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	The Organization reported that the likelihood of significant harm resulting from this incident is "unknown". 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 ransom demand).

between the incident and the possible harm.	The Organization also reported that personal files were "downloaded" although the Organization cannot confirm this, and the Organization reported that it does not know when the breach first occurred.

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, financial, employment and health information potentially at issue could be used to cause the harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. These are all significant harms. Because the Organization cannot confirm whether other personal information might have been accessed, it is not clear what other possible harms may exist.

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 ransom demand). The Organization also reported that personal files were "downloaded" although the Organization cannot confirm this, and the Organization reported that it does not know when the breach first occurred.

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).

The Organization is required to confirm to my Office in writing, within ten (10) days of the date of this decision, that any additional affected individuals whose information is in the control of the Organization have been notified of this incident in accordance with the requirements outlined in the Regulation.

Jill Clayton
Information and Privacy Commissioner