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	Apeetogosan (Metis) Development Inc. (Organization)
Decision number (file number)	P2020-ND-113 (File #014227)
Date notice received by OIPC	December 17, 2019
Date Organization last provided information	April 6, 2020
Date of decision	September 25, 2020
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 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, • address, • date of birth, • social insurance number, and • tax information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from individuals by telephone. To the extent the personal information was collected in Alberta, PIPA applies in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On December 3, 2019, the Organization found its computer system was affected by a ransomware attack that caused its files to be encrypted. The attacker demanded a ransom. • The Organization reported its computer system risk management process includes backup systems and data, so the majority of the system and data were not subject to the attack. The Organization did not pay the ransom. • Due to the nature of the attack and the short time between becoming aware of the attack and restoring its computer systems, the Organization cannot say with certainty that no digital files were downloaded by the third party from its server.
Affected individuals	The incident affected 275 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Ensured that all computers are running the Windows updates. • Notified the Edmonton Police Service.
Steps taken to notify individuals of the incident	Affected individuals were notified of the incident in writing on December 24, 2019.
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 that the "Stolen identities" is a possible harm that may occur as a result of the breach In my view, a reasonable person would consider the contact, identity and financial information 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 provide an assessment of the likelihood that significant harm would result from this incident but it did report "We do not know if the criminals uploaded any of our data but of course it is entirely possible." 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). The Organization was able to restore data and functionality from backups; however, the Organization cannot say with certainty that no digital files were downloaded by the third party from its server.

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 and financial information 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 ransom demand). The Organization was able to restore data and functionality from backups; however, the Organization cannot say with certainty that no digital files were downloaded by the third party from its server. 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 in writing on December 24, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner