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	Datatax Business Services Limited (Organization)
Decision number (file number)	P2021-ND-201 (File #019251)
Date notice received by OIPC	February 3, 2021
Date Organization last provided information	July 15, 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 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 incident involved all or some of the following information: • name, • address, • social insurance number, and • bank account number. 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 December 18, 2020, the Organization was victim to a ransomware (MountLocker) attack that infected several PCs and servers. • The incident was discovered the same day when staff found anomalous files on their computers.

	• The Organization was unable to determine the cause or entry point of the attack.
Affected individuals	The incident affected 6,100 of individuals, including 2,158 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately shut down all systems and forced a password reset for all users. • Reported the incident to police authorities. • Offered identity theft monitoring to affected individuals. • Hired a third party IT services provider to quarantine affected systems. • Hired a firm to investigate the incident. • Monitoring dark web activity. • Recalled all hardware from users and replaced storage drives or entire computers. • Implemented multi-factor password authentication systems. • Implemented a 24/7 monitoring service. • Reviewing and improving data handling protocols. • Hardened network as recommended by IT provider. • Providing additional staff training on the recognition and prevention of phishing and cyber attacks.
Steps taken to notify individuals of the incident	Affected individuals were notified by email and/or letter on February 5, 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 "individual identity theft". In my view, a reasonable person would consider that the contact, identity, and financial information at issue could be used to cause the significant harms of identity theft or 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: *Through our investigation we uncovered no evidence that data was extracted, however the files were encrypted making it possible that the information was accessed and exported. Based on our experience to date post incident, our assessment and the likelihood of harm is low. We have had no reports of individuals experiencing any issues due to this incident.*

	In my view, 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 installation of ransomware). Further, while the Organization has no reports of individuals experiencing issues, it could not rule out the possibility that information was exported. Identity theft or fraud may occur months or years after a breach.

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 at issue could be used to cause the significant harms of identity theft or 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 installation of ransomware). Further, while the Organization has no reports of individuals experiencing issues, it could not rule out the possibility that information was exported. Identity theft or fraud may occur months or years after a breach.

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 email and/or letter on February 5, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner