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	Frederick W. Howarth III d/b/a TBG West Insurance Services (Organization)
Decision number (file number)	P2021-ND-026 (File #016521)
Date notice received by OIPC	July 24, 2020
Date Organization last provided information	July 24, 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 is located in Culver City, CA, USA, and is a broker for disability, long-term care, and group life insurance coverage. 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 includes all or some of the following: • name, • date of birth, and • social insurance number. 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	• On March 27, 2020, the Organization learned that its computer system was impacted by a ransomware event that encrypted certain files. Some files were copied from the system in connection with the attack.

	• On or about June 10, 2020, the Organization determined that a limited number of documents that may have been copied contained some personal information. • The Organization reviewed the contents of all files that may have been acquired. As the Organization could not definitively rule out that the files were accessed, it identified all of the individuals whose personal information was contained in the files on the system.
Affected individuals	The incident affected 41 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Reset employees' passwords. • Retained a forensic security firm to investigate and confirm the overall security of email and computer systems. • Notified the FBI on March 31, 2020. • Through purchasing the decryption key from the threat actor, was able to restore all of the encrypted data on its network. • Installed end-point monitoring protection during the forensic investigation. • Engaged with an outside vendor for additional security monitoring and continued end-point monitoring tool for 24/7 monitoring of its computer environment. • Moved its Exchange server. • Informed affected individuals of steps they can take to protect themselves and offered complimentary dark web monitoring services.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter between July 23 and July 30, 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 the possible harm that may occur as a result of the breach is "financial harm." In its notice to affected individuals, the Organization said, "Although we are not aware of any instances of fraud or identity theft, we are offering a complimentary one-year membership." In my view, a reasonable person would consider the identity information (including social insurance number and date of birth) at issue could be used to cause the significant harms of identity theft, fraud, and financial loss.

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, *Given that the threat actor copied certain files from [the] system, there is a possible likelihood of harm to the impacted individuals, including the possibility of financial fraud.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because it resulted from the malicious action of an unknown third party, who made a ransom demand. The Organization also reported some files were copied and it cannot rule out that the files were accessed.

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 identity information (including social insurance number and date of birth) at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. The likelihood of harm resulting from this incident is increased because it resulted from the malicious action of an unknown third party, who made a ransom demand. The Organization also reported some files were copied and it cannot rule out that the files were accessed.

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 between July 23 and July 30, 2020 in accordance with the Regulation. The Organization is not required to notify these affected individuals again.

Jill Clayton
Information and Privacy Commissioner