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	Arthur J. Gallagher Canada Limited (AJG Canada) and Gallagher Bassett Canada Inc. (GB Canada) (together the Organization).
Decision number (file number)	P2022-ND-028 (File #022199)
Date notice received by OIPC	July 15, 2021
Date Organization last provided information	January 14, 2022
Date of decision	May 2, 2022
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"	AJG Canada provides insurance brokerage services. It is a subsidiary of Arthur J. Gallagher & Co. ("AJG"), a US-based entity that provides insurance brokerage, risk management and consulting services globally. GB Canada provides insurance claims management services to a number of insurance companies. As such, it processes claims information, which includes personal data. GB Canada is also a subsidiary within the AJG group. GB Canada is also reporting the incident on behalf of Hartford Fire insurance Company and on behalf of L Brands. 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 details, • date of birth, • bank account or payment card information, • claim / policy number, • health insurance information,

	• medical information, • digital signature, • employment ID number, and • passport or social insurance numbers, biometric data or other identification information (in a limited number of cases). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies. The Organization reported, "No biometric information was involved in the case of Canadian residents."
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On 26 September 2020, the Organization detected a ransomware event effecting its internal systems. • The Organization's investigation determined that an unauthorized party accessed or acquired data contained within certain segments of its network between June 3, 2020 and September 26, 2020. • The Organization was able to confirm that certain systems were accessed but it was unable to confirm what information within those systems was, in fact, accessed. • The Organization has no evidence of any actual or attempted misuse of the information related to this incident.
Affected individuals	The incident affected 47,241 individuals and approximately 1073 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Isolated impacted systems and enacted business continuity and incident response plans. • Worked with external security experts. • Assessed the security and viability of its backups to ensure they were not infected with ransomware or other malware and restored access and operations of impacted systems via clean backups. • Mobilized the incident response team and launched an investigation into the incident and its impact on the accessibility and security of both its systems and data. • Reviewed existing security policies. • Implementing additional measures and enhanced security tools. • Reported to law enforcement and regulatory bodies. • Notified its affected clients.

	• Offered affected individuals identity and credit monitoring services for 24 months and established a dedicated call centre. • Continuing to monitor network for any unauthorized activity. No evidence found of ongoing unauthorized access. • Ongoing dark-web monitoring in place.
Steps taken to notify individuals of the incident	AJG Canada notified affected individuals starting on October 19, 2021 and again on December 16, 2021. GB Canada notified its clients on behalf of whom it processed the information. For those clients who opted in to the notification process, GB Canada notified the affected individuals involved on their behalf on September 3, 2021, November 9, 2021, and November 24, 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 did not specifically identify any harm that might result from this incident. However, its notification to affected individuals stated, *…we are offering you, at no cost, identity and credit monitoring services for 24 months. Information and instructions on how to enroll in these free services can be found in the "Steps you can take to help protect your information" section below, as well as additional steps you can take to increase the protection of your data.* In my view, a reasonable person would consider the contact, identity, financial, employment and medical information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The medical information at issue could also be used to cause hurt, humiliation or embarrassment.
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, *Although the organization has no evidence of any actual or attempted misuse of information, and has no indication the information is in the possession or control of an unauthorized person or party, it is reporting the Incident and informing the affected individuals as well as its clients on behalf of whom it processes data out of an abundance of caution and to make them aware of the incident.* 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 (ransomware demand). In addition, the

	Organization reported that the personal information at issue was accessed or acquired during a four-month period. Additionally identity theft and fraud can happen months and even years after a data 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 the contact, identity, financial, employment and medical information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The medical information at issue could also be used to cause hurt, humiliation or embarrassment.

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 (ransomware demand). In addition, the Organization reported that the personal information at issue was accessed or acquired during a four-month period. Additionally identity theft and fraud can happen months and even years after a data 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 on September 3, 2021, October 19, 2021, November 9, 2021, November 24, 2021 and on December 16, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance