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	Worldwide Insurance Services, LLC (Organization)
Decision number (file number)	P2021-ND-112 (File #008736)
Date notice received by OIPC	May 22, 2018
Date Organization last provided information	May 22, 2018
Date of decision	March 31, 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 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 administers international health insurance products on behalf of health insurance companies and company health products and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved some or all of the following information: • name of member, • date of birth, • health plan member ID number, and • claims information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization says that "This report is not, and does not constitute, a waiver of [the Organization's] objection that Alberta lacks personal jurisdiction regarding the company related to this matter"; however, the Organization did not explain why it believes this to be the case. In my view, the Organization is an "organization" as defined in PIPA, and the information at issue is "personal information" as defined in PIPA. To the extent the personal information was collected in Alberta by the Organization, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• Following an investigation of a suspected security incident, the Organization determined that, between October 11 - 13, 2017, an unauthorized party may have obtained credentials to two employee email accounts through a phishing email scheme. • As a result, the unauthorized party may have obtained access to emails and attachments in the employees' email accounts. • After reviewing the emails within the accounts, the Organization determined that emails in one account contained information about 8 health plan members who are residents of Alberta. • Although no evidence was found during the investigation that indicated that any emails in the employees' accounts were in fact acquired or accessed, the Organization cannot rule out the possibility. • The incident was discovered March 23, 2018.
Affected individuals	The incident affected eight (8) health plan members who are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Initiated an internal investigation. • Provided training for employees regarding phishing emails and other cybersecurity issues. • Enhanced existing security measures by installing software to detect phishing emails and prevent their receipt by employees and also implemented multi-factor authentication for remote access to email. • Notified health insurance companies and company health plans with potentially affected members and offered to provide notice to those members and applicable regulatory agencies on their behalf.
Steps taken to notify individuals of the incident	The Organization reported that affected individuals were notified beginning on May 21, 2018.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 "To date, [the Organization] has no indication that any member information was actually accessed or misused. However, out of an abundance of caution, and to reduce the risk of identity theft, [the Organization] has provided notice to all potentially affected members and has advised them to regularly review the explanation of benefits received from their health insurer. No social insurance numbers or financial information belonging to Alberta residents was found in the employee's email account, so the risk of financial loss or fraud is minimial [sic]."

	In my view, a reasonable person would consider that the identity information at issue (date of birth, health plan ID), particularly combined with claims information, could be used to cause the significant harms of identity theft and fraud, as well as potentially hurt, humiliation and 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 did not specifically address the likelihood of harm resulting from this incident, but did report "To date, [the Organization] has no indication that any member information was actually accessed or misused. However, out of an abundance of caution, and to reduce the risk of identity theft, [the Organization] has provided notice to all potentially affected members and has advised them to regularly review the explanation of benefits received from their health insurer." In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing email and compromised credentials) and the information was exposed over a period of three days.

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 as a result of this incident.

The identity information at issue (date of birth, health plan ID), particularly combined with claims information, could be used to cause the significant harms of identity theft and fraud, as well as potentially hurt, humiliation and embarrassment. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing email and compromised credentials) and the information was exposed over a period of three days.

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 affected individuals were notified beginning on May 21, 2018. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner