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	The Commonwell Mutual Insurance Group (Organizations)
Decision number (file number)	P2021-ND-271 (File #020864)
Date notice received by OIPC	May 3, 2021
Date Organization last provided information	November 19, 2021
Date of decision	February 11, 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 the 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 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 the following information: Current and former members: • name, • age, • home address, • home telephone number, • banking information, • driver's license, and • driver's abstract. Current or former employees: • name, • salary, • age, • banking information, • home address, • home telephone number, • education history, • RRSP account information, • employment history (offer, promotion and termination letters), and disciplinary and performance information.

	Third parties involved in claims or litigation: • name, • home address, • financial information, • employment information, • driver's history, • medical information (clinical notes and records, medical reports, OHIP summaries, prescription summaries). 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.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On March 3, 2021, the Organization became aware that an unauthorized third party had gained access to its IT system on February 24, 2021. • The Organization reported that the unauthorized third party was able to gain access to elevated privileges and launch Cobalt Strike. Some registries were modified and suspicious files were created on the system. • On March 26, 2021, the Organization learned that certain personal information may have been exfiltrated. • All internal systems were operational and there was no encryption of data or interruption of services. • The Organization reported the "root cause of the incident could not be determined, but the unauthorized third party likely gained access to the … environment via VPN connection."
Affected individuals	The incident affected approximately 275,000 individuals including 287 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Provided complimentary identity theft and credit monitoring solutions, free of charge for 12 months. • Retained the services of cyber forensic experts to investigate. • Retained the services of a cybersecurity firm to monitor the dark web. • Notified local police and relevant authorities. • Taking a number of additional measures to strengthen systems.

Steps taken to notify individuals of the incident	Current and former employees and current and former members who were affected by the incident were notified by letter, which started on May 3, 2021. The Organization reported, *As for the potentially affected third parties involved in claims or litigation, [the Organization] is working with an external vendor that is currently assisting with document review to identify potentially affected individuals in order to notify them. This exercise is ongoing, given the size and volume of data to process, and should be completed by the end of the month. The notifications to approximately 2,000 individuals are expected to be sent out the following two weeks after completion of the review.*
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 "Some of the personal information may be used to conduct identity theft, to conduct fraudulent banking activities, and for future phishing attempts." In my view, a reasonable person would consider that that the contact, identity, financial and employment information at issue could be used to cause the harms of identity theft, fraud, and/or financial loss. Medical information could be used to cause the significant harms or humiliation and embarrassment. Email addresses (if at issue) could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms.
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, *Low likelihood. There is currently no evidence that the personal information is being misused.* In my view, a reasonable person would consider that 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). The lack of evidence that the information "is being misused" is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach. In this case, the personal information was exposed for approximately a month before the Organization learned it may have been exfiltrated.

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 that the contact, identity, financial and employment information at issue could be used to cause the harms of identity theft, fraud, and/or financial loss. Medical information could be used to cause the significant harms or humiliation and embarrassment. Email addresses (if at issue) could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms.

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). The lack of evidence that the information "is being misused" is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach. In this case, the personal information was exposed for approximately a month before the Organization learned it may have been exfiltrated.

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 current and former employees and members who were affected by the incident starting on May 3, 2021, in accordance with the Regulation. The Organization is not required to notify these affected individuals again.

The Organization reported that it was "working with an external vendor" to identify potentially affected third parties involved in claims or litigation and expected notifications to be sent to approximately 2,000 individuals.

I require the Organization to confirm to my office in writing, within 10 days of the date of this decision, that all affected individuals for whom there is a real risk of significant harm and whose personal information was collected in Alberta, have been notified in accordance with section 19.1 of the Regulation.

Jill Clayton
Information and Privacy Commissioner