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	Blue Cross Life Insurance Company of Canada (Organization)
Decision number (file number)	P2021-ND-258 (File #020861)
Date notice received by OIPC	May 6, 2021
Date Organization last provided information	July 23, 2021 (supplemental report)
Date of decision	January 31, 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"	The Organization is an "organization" as defined in section 1(1)(i) of PIPA. The Organization reported "Although it appears likely that the affected personal information was all under the control of Saskatchewan Blue Cross, [the Organization] is filing this report out of an abundance of caution given that the investigation of the matter is ongoing".
Section 1(1)(k) of PIPA "personal information"	The Organization uses a third party, Saskatchewan Blue Cross (SBC), to provide claim adjudication and case management services for life and disability products underwritten by the Organization. SBC provides these services through its wholly owned subsidiary BlueCo Services Inc. SBC submitted a related breach report to this office. That report identified four categories of personal information relating to Albertans potentially affected by this incident. Only the following two categories of affected personal information relate to products underwritten by the Organization. <u>Personal information about a SBC individual's disability claim including:</u>

	• name, • address, • telephone number, • email address, • policy number, • premium amount, • claim amount, • health information, • date of birth, • family status, • salary, • health card number, • government issued ID, and • in some instances, credit card information, banking information and/or social insurance number. <u>Personal information about certain members of Medavie Blue Cross, where such information is shared between processes as a part of collaboration to serve members:</u> • name, • address, • telephone number, • email address, • certificate number, • policy number, • premium amount, • claim amount, • health information, • date of birth, and • salary. The above is information 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 April 20, 2021, SBC discovered it was the victim of a ransomware incident that resulted in the encryption and unauthorized access to certain of its systems. • On April 23, 2021, SBC advised the Organization that personal information relating to its disability claims might have been affected.

	• On May 4, 2021, SBC advised the Organization that information relating to life and disability claims was accessed and provided an initial indication of the number of affected individuals. • The Organization reported that its network and systems are separate from those of SBC and there is no indication that the Organization's systems were accessed or compromised. • The Organization reported that SBC's investigation determined that the root cause of the incident and compromise of its systems was likely through a phishing email, although the root cause of the incident cannot be conclusively determined. • SBC informed the Organization that a third party threat actor had unauthorized access to certain of SBC's systems between approximately April 6, 2021 and April 20, 2021.
Affected individuals	The incident affected approximately 494 individuals in Alberta under categories 2 and/or 4.
Steps taken to reduce risk of harm to individuals	• Initiated incident management process. • Assembled an Assessment Team. • Blocked communication from the SBC network to the Organization's systems, email, and network. • Initiated a process to continue paying/processing claims to all life/disability claimants in order to minimize the financial impact to claimants. • Notified the Office of the Privacy Commissioner of Canada, the Office of the Superintendent of Financial Institutions, and the Financial and Consumer Affairs Authority of Saskatchewan. • Worked with SBC to provide notice to affected individuals and offered identity theft and credit monitoring services for a period of twenty four (24) months, where it was determined that there exists a real risk of significant harm.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on July 23, 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, *In light of the nature of the Incident and the type of personal information involved, the potential harms that may occur to the affected Alberta individual as a result of the Incident could include hurt, humiliation or embarrassment.* In my view, a reasonable person would consider the contact, identity, financial, insurance, medical and employment information at issue could be used to cause the significant harms of identity theft, fraud, financial loss and embarrassment. Email

	addresses 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 it "agrees with SBC's assessment that the likelihood of harm to affected individuals is low." 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, ransom demand). The lack of evidence that the personal information has been misused is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach. Although SBC has enhanced safeguards, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information accessed from SBC's systems were to be used for fraudulent purposes, for example. Further, the information may have been available to the unauthorized third party for approximately two (2) weeks.

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, insurance, medical and employment information at issue could be used to cause the significant harms of identity theft, fraud, financial loss and embarrassment. Email addresses 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, ransom demand). The lack of evidence that the personal information has been misused is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach. Although SBC has enhanced safeguards, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information accessed from SBC's systems were to be used for fraudulent purposes, for example. Further, the information may have been available to the unauthorized third party for approximately two (2) weeks.

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 July 23, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner