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** | Saskatchewan Blue Cross (Organization) |
| **Decision number (file number)** | P2021-ND-260 (File #020863) |
| **Date notice received by OIPC** | May 6, 2021 |
| **Date Organization last provided information** | July 23, 2021 |
| **Date of decision** | February 8, 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. |
| **Section 1(1)(k) of PIPA "personal information"** | The incident involved all or some of the following information:<br><br><u>Category #1</u> - Personal information about certain members of the Organization who reside in Alberta:<br><br>• name,<br>• address,<br>• telephone number,<br>• email address,<br>• policy number,<br>• premium amount,<br>• claim amount,<br>• health information,<br>• date of birth,<br>• family status,<br>• salary,<br>• health card number,<br>• government issued ID, and<br>• in some instances, credit card information, banking information and/or social insurance number. |

| | |
|---|---|
| | Category #2 – Personal information about a member's disability claim:<br><br>• name,<br>• address,<br>• telephone number,<br>• email address,<br>• policy number,<br>• premium amount,<br>• claim amount,<br>• health information, and<br>• date of birth.<br><br>In some instances related only to the Organization's members, the information may also include:<br><br>• family status,<br>• salary,<br>• health card number,<br>• government issued ID, and<br>• in some instances, credit card information, banking information and/or social insurance number.<br><br>The Organization, through its wholly owned subsidiary, BlueCo Services Inc., provides claim adjudication and case management services for life and disability products underwritten by Blue Cross Life Insurance Company of Canada (BCL). Pursuant to the Organization's written agreement with BCL this information was in the custody and control of the Organization at the time of the incident.<br><br>Category #3 – The Organization additionally processes certain health and wellness claims for other Canadian Blue Cross organizations. As such, the Organization's investigation into the incident determined that the personal information of Alberta residents who are members of one of the other Canadian Blue Cross organizations other than Alberta Blue Cross may be at issue, including some combination of the following personal information:<br><br>• name,<br>• address,<br>• telehone number,<br>• email address,<br>• policy number,<br>• premium amount,<br>• claim amount,<br>• health information, |

| | |
|---|---|
| | • date of birth,<br>• family status,<br>• health card number and/or government issued ID, and<br>• in some cases pertaining only to Medavie Blue Cross, salary and social insurance number.<br><br><u>Category #4</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:<br><br>• name,<br>• address,<br>• telephone number,<br>• email address,<br>• certificate number,<br>• policy number,<br>• premium amount,<br>• claim amount,<br>• health information,<br>• date of birth, and<br>• salary.<br><br>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 April 20, 2021, the Organization discovered it was the victim of a ransomware incident that resulted in the encryption of, and unauthorized access to, certain of its systems.<br>• The Organization determined that the incident was perpetrated by a third party threat actor that exfiltrated certain categories of data.<br>• The Organization's investigation also 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.<br>• The Organization reported that it determined that the third party threat actor had unauthorized access to certain systems from approximately April 6, 2021 until April 20, 2021. |

| | |
|---|---|
| **Affected individuals** | The incident affected approximately 1,278 Alberta residents. |
| **Steps taken to reduce risk of harm to individuals** | • Engaged a specialized forensic IT company to conduct an investigation to determine the cause and scope of the incident and took immediate steps to contain and remediate any impacts from the Incident.<br>• Arranged to offer identity theft and credit monitoring services to all affected individuals for whom it has determined that there exists a real risk of significant harm for a period of twenty four (24) months.<br>• Reviewing privacy and cybersecurity safeguards, policies, procedures and measures to consider whether further improvements are recommended.<br>• Notified the Office of the Superintendent of Financial Institutions as well as Regional Blue Cross Organizations, including Alberta Blue Cross.<br>• Provided information to the Financial and Consumer Affairs Authority of Saskatchewan.<br>• Notified law enforcement and the Office of the Federal Privacy Commissioner of Canada.<br>• Conducting ongoing dark web monitoring to determine ongoing signs of misuse of any data potentially compromised in the incident. |
| **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**<br>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<br><br>*In light of the malicious nature of the Incident and the type of personal information involved; the potential harms of fraud, identity theft, financial loss, hurt, humiliation and embarrassment may occur as a result of the Incident.*<br><br>I agree with the Organization's assessment. A reasonable person would consider the contact, identity, financial, health 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**<br>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 its assessment that ….<br><br>*… the likelihood of harm to affected individuals is low. [The Organization] has no evidence that the personal information at issue has been misused or distributed by the third party threat actor and based on the steps taken …to date in responding to the Incident, it believes the risk of further access or disclosure of the compromised personal information is low.*<br><br>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 the Organization has put additional safeguards in place, 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 the Organization'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, health 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 the Organization has put additional safeguards in place, 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 the Organization'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