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** | Mosaic Primary Care Network (Organization) |
| **Decision number (file number)** | P2020-ND-037 (File #014268) |
| **Date notice received by OIPC** | March 9, 2020 |
| **Date Organization last provided information** | March 13, 2020 |
| **Date of decision** | March 30, 2020 |
| **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 operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA. |
| **Section 1(1)(k) of PIPA "personal information"** | The Organization reported the incident involved information of its staff/employees and those of Highland PCN, and Calgary Rural PCN:<br><br>• full name,<br>• demographic information (name, address, email address),<br>• financial information (bank name, account numbers),<br>• salary information,<br>• Social Insurance Number.<br><br>The following individually identifying health information is also at issue:<br><br>• full name,<br>• demographic information (name, address, email address),<br>• date of birth,<br>• personal health number,<br>• health services provider information,<br>• amounts billed,<br>• treatment dates,<br>• treatment / diagnostic information (consult notes) |

| | |
|---|---|
| | According to its website, the Organization is "a group of family doctors and healthcare professionals that provide primary health care, in partnership with Alberta Health Services".<br><br>To the extent the information at issue in this matter is health information as defined in Alberta's *Health Information Act* (HIA), PIPA does not apply (section 4(3)(f)).<br><br>However, to the extent the information at issue in this matter is not "health information" as defined in HIA, but is nonetheless "personal information" as defined in section 1(1)(k), PIPA applies. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |
| **Description of incident** | • An employee's email account was compromised and used to impersonate an external software vendor. As a result, a payment sent from the Organization to the vendor was sent to a fraudulent bank account.<br>• The breach was discovered on December 10, 2019 when the Organization's employee informed the IT department of suspicious activity. The IT department identified that the user's password was likely compromised through phishing.<br>• The cyber-attack was found to have exposed the MS 365 cloud environment and but no other systems.<br>• The Organization's investigation identified a total of four (4) email inboxes that were exposed. |
| **Affected individuals** | The incident affected 70,000+ individuals. |
| **Steps taken to reduce risk of harm to individuals** | • Initiated an internal investigation and engaged an external auditor.<br>• Reset passwords and implemented two-factor authentication.<br>• Reminded physicians of approved information transfer protocols.<br>• Sent staff an email outlining steps to deal with the breach and actions to undertake including privacy training and review of privacy policies<br>• Reviewed accounts for password strength, discontinued inactive accounts, increased password complexity requirements.<br>• Activated additional security features.<br>• Reviewing internal IT processes and expanding reporting.<br>• Expanding staff education program to include ongoing IT/cyber security awareness training. |

| | |
|---|---|
| | • Offered credit monitoring to affected individuals. |
| **Steps taken to notify individuals of the incident** | The Organization reported that it notified its staff and member physicians, as well as those of Highland PCN, and Calgary Rural PCN, and 13 individuals initially identified as being affected, by email and registered mail between December 30, 2019 and February 26, 2020.<br><br>The Organization also requested "authorization to provide notice through substitutional services to remaining individuals with exposed individually identifying health information". |
| **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 that "The possible risks of harm include financial loss, identity theft, fraud, and possible damage to reputation".<br><br>I agree with the Organization's assessment. A reasonable person would consider that the contact, identity, employment, financial and health information at issue could be used to cause the harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. Email addresses could be used for phishing purposes, 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 that "The breach was the result of cybercrime, and we determine that there is a risk of harm. Mitigating factors include that the cyber-attack likely targeted a specific financial transaction and that technical safeguards were in place at the time of the incident…".<br><br>In my view, a reasonable person would consider that the likelihood of harm is increased because the incident resulted from malicious intent (cybercrime with fraudulent intent) and payment was sent to a fraudulent account. |
| **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.<br><br>A reasonable person would consider that the contact, identity, employment, financial and health information at issue could be used to cause the harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are all significant harms. | |

The likelihood of harm is increased because the incident resulted from malicious intent (cybercrime with fraudulent intent) and payment was sent to a fraudulent account.

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). Section 19.1(1) of the Regulation states that the notification must "… be given directly to the individual…" , although section 19.1(2) says "… the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

In this case, the Organization reported that it notified its staff and member physicians, as well as those of Highland PCN, and Calgary Rural PCN, and 13 individuals initially identified as being affected, directly by email and registered mail between December 30, 2019 and February 26, 2020.

The Organization also requested "… authorization to give notice by substitutional service due to 1) a projected very high number of affected individuals (likely >70,000), 2) barriers to contacting affected individuals, 3) added risks related to identifying the contact information of affected individuals, and 4) restrictions on timely notifications". This request was for notification to affected "individuals with compromised individually identifying health information".

The Organization said that indirect notice would be given by various methods, including via its website and posters/signs at member clinics, and support would be provided to affected individuals through email and telephone.

I reviewed the Organization's submissions and accept that indirect or substitute notice as described by the Organization is reasonable in this case. **I require the Organization to provide written confirmation to my Office of its efforts to indirectly notify affected individuals, within 20 days of the date of this decision.**

Jill Clayton
Information and Privacy Commissioner