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)	P2021-ND-193 (File #017989)
Date notice received by OIPC	November 12, 2020
Date Organization last provided information	June 15, 2021
Date of decision	October 14, 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 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 incident involved all or some of the following information: • name, • email address, and • telephone number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On October 17, 2020, a shared administrative user account was used to gain unauthorized access to the Organization's Office 365 SharePoint site (and linked files). • An audit log review revealed that the threat actor accessed, viewed, and downloaded files, and uploaded a file (an image file – ransomware.jpg) from/to the Organization's SharePoint site. User accounts were also removed from the site. • The breach was discovered on October 17, 2020.

Affected individuals	The incident affected nine residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Breached account was disabled, and password reset. • Deleted SharePoint site, including all associated files. • Notified affected individuals and provided them with information on how to protect themselves from potential cybercrime. • Notified law enforcement. • Reviewing all accounts with more than one device linked to receive 2FA. • Strengthening the employee off-boarding process to ensure that all devices for a user are reassigned, deleted, reset and/or removed from Organization systems. • Strengthening onboarding process to ensure that appropriate equipment is available to new staff. • Strengthening documentation of changes to user accounts to ensure that all changes are logged so that they can be undone quickly in the event of staff departure. • Providing additional training to IT administrators on the management of Office 365. • Implementing additional log management software tools to increase monitoring abilities.
Steps taken to notify individuals of the incident	Affected individuals were initially notified by telephone between November 2–10, 2020. Follow-up notification emails were sent to affected individuals between November 6 – 10, 2020.
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: *Possible harms that may result from this breach are related to potential phishing, malware, and/or social engineering attacks as the cybercriminal has gained access to the affected individuals' email addresses and phone numbers.* In my view, a reasonable person would consider that the contact information at issue, including email address, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are 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: *The breach was the result of cybercrime, and we therefore determine that there is a risk of harm. Mitigating factors include that the exposure of the information was limited to a 4-hour time window (until the password was reset and the account disabled). The account had limited assigned privileges and as such, the cybercriminal was only able to access one SharePoint site/files associated with one MPCN project, as described above.* I agree with the Organization's assessment. A reasonable person would consider 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) and information was 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 the contact information at issue, including email address, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are 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) and information was 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 affected individuals by telephone and email between November 2-10, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner