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	Medical Pharmacies Group Limited (Organization)
Decision number (file number)	P2022-ND-008 (File #022379)
Date notice received by OIPC	October 8, 2021
Date Organization last provided information	October 8, 2021
Date of decision	March 23, 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 headquartered in Markham, Ontario, 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, • mailing address, • email address, • telephone number, • social insurance number, • date of birth, • employment information, • employment benefits information, • payroll information, and • banking information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On May 22, 2021, the Organization was victim to a ransomware attack. The incident was discovered the same day by the Organization's IT personnel. • An investigation determined that the attacker my have gained access to personal information of current and former employees. • The Organization did not report how the attacker compromised and gained access to their network.
Affected individuals	The incident affected 3,374 individuals, including 78 whose personal information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Forced password resets. • Enhanced certain IT security practices. • Updated data retention policies. • Searched the Dark Web for evidence of leaked data. • Offered cybersecurity awareness training for employees. • Provided affected individuals with identity and credit monitoring services. • Notified law enforcement.
Steps taken to notify individuals of the incident	Affected current employees were notified by email on August 19, 2021. Affected former employees were notified by letter on September 28, 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 that "There is a risk of identity theft, fraud and phishing attempts as well as hurt humiliation and embarrassment." I agree with the Organization's assessment. A reasonable person would consider that the identity (date of birth, social insurance number), employment, and financial information at issue could be used to cause the harms of identity theft, fraud, and possibly hurt, humiliation, and embarrassment. Email addresses 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 likelihood that harm could result is low. We understand from the forensic investigation that Dark Web searches reveal no evidence that [the Organization's] data was leaked. Additionally, identity theft and credit monitoring has been offered to potentially affected individuals.* Notices provided to affected individuals stated: *[The Organization is] unable to confirm with certainty whether or not your information was affected, and we want to stress that we are not aware of any misuse of this information.* 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 unauthorized third party (deliberate intrusion and deployment of ransomware). A lack of evidence that records have been "leaked" or misused does not mitigate against future harm as records can be published and misused months or years after a breach. Further, the Organization did not rule out, with certainty, the possibility that records were 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 identity (date of birth, social insurance number), employment, and financial information at issue could be used to cause the harms of identity theft, fraud, and possibly hurt, humiliation and embarrassment. Email addresses 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 unauthorized third party (deliberate intrusion and deployment of ransomware). A lack of evidence that records have been "leaked" or misused does not mitigate against future harm as records can be published or misused months or years after a breach. Further, the Organization did not rule out, with certainty, the possibility that records were 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 email or letter on August 19, 2021 and September 28, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance