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	Debra Jackson, Registered Psychologist (Organization)
Decision number (file number)	P2022-ND-015 (File #022137)
Date notice received by OIPC	July 5, 2021
Date Organization last provided information	January 21, 2022
Date of decision	April 1, 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 the 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 some or all of the following information: • name, • contact information, • patient information. 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 March 4 or 5, 2021, an employee responded to a phishing email that purported to be from Microsoft. • On March 8, 2021, the employee's email account was hijacked and the employee's contacts were sent emails requesting they purchase gift cards. • The Organization was notified by the employee's contacts that they were receiving emails from the employee about gift cards.

Affected individuals	The incident affected approximately 207 individuals.
Steps taken to reduce risk of harm to individuals	• Hired a cyber security firm to perform an e-Discovery of the contents of the email inbox. • Identified patients whose information was exposed. • Changed employee's email credentials. • Notified affected individuals to ignore any emails coming from the affected email account. • Became more aware of the types of phishing scams being employed by threat actors. • Initiated the use of double factor authentication on most accounts.
Steps taken to notify individuals of the incident	Affected individuals were notified in person or by email on July 20, 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, *Patients' information was exposed to the attacker along with their contact information.* In my view, a reasonable person would consider that the contact and medical information at issue could be used to cause the significant harms of hurt, humiliation or embarrassment. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to financial loss and fraud.
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, *No client has been approached since (the employee) mitigated the attack by changing her email credentials. It would appear that the attacker, being from Nigeria, was only interested in trying to get (the employee's) contacts to purchase gift cards.* 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 . The lack of reported incidents is not a mitigating factor as the identifmalicious action of an unknown third party (deliberate intrusion into an employees' email account)ied harms can happen months and even years after a data breach.
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 and medical information at issue could be used to cause the significant harms of hurt, humiliation or embarrassment. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to financial loss and fraud.

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 into an employees' email account). The lack of reported incidents is not a mitigating factor as the identified harms can happen months and even years after a data breach.

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 in person or by email on July 20, 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