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	Canadian Medical Association (Organization)
Decision number (file number)	P2021-ND-175 (File #017957)
Date notice received by OIPC	November 4, 2020
Date Organization last provided information	November 4, 2020
Date of decision	August 27, 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 the individual 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 Organization reported the incident involved some or all of the following information for one Alberta resident: • name, • work email address, • home address, • social insurance number and • banking institution name and account number. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• Between October 6 -21, 2020, as the result of a phishing incident, email messages received in an employee's inbox were forwarded to an unknown webmail account. • The incident was discovered on October 21, 2020 by the Organization's IT team.

	• Several employees received the message, but only one employee clicked on the "attachment". • The Organization reported it not aware of any incidents of unauthorized use of the information at issue, and the Organization's data breach monitoring solution has not identified any attempts to traffic the disclosed data.
Affected individuals	The incident affected 37 individuals, including 1 Alberta resident.
Steps taken to reduce risk of harm to individuals	• Immediately disabled all accounts for the affected employee. • Posted a website notice advising of the incident and providing contact details for the Organization. • Strengthened password policies for user accounts • Reviewed access controls to administrative systems used by the Organization. • Ongoing forensic review. • Reviewed existing security suite and controls to identify potential areas for augmentation, including email encryption and employee threat alerts. • Provided refresher training to all employees. • Arranged a one-year subscription to an online monitoring service, at no cost. • Contacted vendors to make them aware of the issue, and notified the appropriate regulatory authorities. • Ongoing web monitoring to detect possible trafficking of the disclosed data continues.
Steps taken to notify individuals of the incident	The affected individual was notified by telephone and letter/ email on October 28, 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… *...there may be a heightened risk of identity theft, given the disclosure of the personal information in question, including SIN. There is also a possible, but lessened identity theft risk for the individuals... We have not identified any possible material harms for the remaining Groups (of individuals).* In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing 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 that it … *… considers the risk of harm is low to medium, given the abbreviated time frame of exposure and the prompt notification and provision of credit monitoring. While for these 8 individuals (which include the one Alberta resident), the disclosed data would generally considered to be "sensitive", on its own, it is unlikely that this data would be particularly useful for identity theft purposes, unless the perpetrators first attempted to collect additional data through social engineering, in order to fill in some of the gaps (other useful identifiers, passwords, etc.) that would make the success of identity theft more likely – a time-consuming endeavour with no guarantees of success and uncertain rewards. Many criminals, who would lean toward seeking low-risk, high-return "quick hits" would be inclined not to try to capitalize on the the (sic) disclosed data, preferring to leverage richer data sets that this episode might produce. The [Organization] does not foresee any real risks of material harm for the individuals in Groups 3 and 4.* 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 into an employee's email account). Although the Organization reported it is not aware of any incidents of unauthorized use of the disclosed information, the lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing/smishing, identity theft and fraud can occur months and even years after a data breach. Further, the information may have been exposed for approximately 3 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 individual.

A reasonable person would consider that the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing 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 into an employee's email account). Although the Organization reported it is not aware of any incidents of unauthorized use of the disclosed information, the lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing/smishing, identity theft and fraud can occur months and even years after a data breach. Further, the information may have been exposed for approximately 3 weeks.

I require the Organization to notify the affected individual 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 the affected individual by telephone and by letter/ email on October 28, 2020, accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner