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)	P2016-ND-35 (File #002908)
Date notice received by OIPC	May 12, 2016
Date Organization last provided information	May 20, 2016
Date of decision	July 7, 2016
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 is a federally incorporated association and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The information at issue includes the following: • name, • email address, and • membership status. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	

Description of incident	• An employee of the Organization received an email request for a list of all Organization members, purportedly from a senior executive in the Organization. • The email appeared to have been sent from a legitimate Organization account, but also requested that the information be sent to a Yahoo account that included the executive's name. The Yahoo account was "spoofed," i.e. fraudulent. • The employee responded to the request, sending the personal information to both the legitimate Organization email account and the spoofed Yahoo account.
Affected individuals	A total of 84,248 Canadians were affected, including 12,449 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• The Organization's IT service provider will block external IP addresses that purport to come from a legitimate Organization account. • Organization employees have been reminded to carefully review email addresses. • The Organization reported the incident to Yahoo.
Steps taken to notify individuals of the incident	Notification to affected individuals sent by email on May 10, 2016.
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 recognized the affected individuals may be at risk for identity theft, as well as possibly "loss of business or employment opportunities." I agree with the Organization's assessment. The information at issue does not include particularly sensitive identity or financial information; however, it does include email addresses. This information could be used to cause the harms of unsolicited emails and phishing. Phishing is a significant harm.
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 considered the likelihood of significant harm resulting from this incident to be "remote". In my view, the likelihood of harm resulting from this incident is increased because the incident resulted from deliberate action (perpetrator impersonated a senior member of the organization), indicating malicious intent, and the circumstances suggest the information at issue was the target.

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. The information at issue does not include particularly sensitive identity or financial information; however, it does include email addresses. This information could be used to cause the significant harm of phishing. The incident resulted from deliberate action (perpetrator impersonated a senior member of the organization), indicating malicious intent, and the circumstances suggest the information at issue was the target. I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified the affected individuals via email on May 10, 2016, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner