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	The Association of Professional Engineers and Geoscientists of Alberta (Organization)
Decision number (file number)	P2015-ND-75 (File #001552)
Date notice received by OIPC	September 21, 2015
Date Organization last provided information	October 27, 2015
Date of decision	November 10, 2015
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"	Organization is an unincorporated association. I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(ii) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, and • email address. This information is about identifiable individuals and qualifies as "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	A new staff member with the Organization received a phishing email, disguised as an email from the Organization's CEO. The email requested members' names and email addresses in Excel format. The staff member responded to the email, including a spreadsheet containing the information at issue.
Affected individuals	A total of 75,000 Albertans were affected.
Steps taken to reduce risk of harm to individuals	• The Organization's Senior Leadership and Council were immediately informed. • The self-service portal that uses email addresses as a user name was temporarily suspended. • Incident response updates were made available on the Organization's website. • A Media Advisory was issued advising members not to respond to emails and not to provide personal information by email.
Steps taken to notify individuals of the incident	Notification sent by email to affected individuals on September 21, 2015.
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 the information at issue is of low to moderate sensitivity, and includes a large percentage of personal email addresses. The potential harms that could result from this incident include further phishing attacks, virus emails, or fraud. Specifically, "the information could be used by third parties for spam, fraud, phishing." I agree with the Organization that the types of harm that could result from this incident include further phishing attacks, virus emails, or 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 assessed there to be a low risk of significant harm to the affected individuals. In my view, the likelihood of harm resulting from this incident is increased because the personal information was specifically targeted by an unauthorised individual, indicating malicious intent. The information has not been recovered.

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 personal information involved could be used to cause the significant harms of phishing attacks, virus emails, or fraud. The information was specifically targeted by an unauthorised individual, indicating malicious intent. The information has not been recovered. 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 members in an email dated September 21, 2015, in accordance with the Regulation. The Organization also issued a public notification and apology in a video posted to a social media site.

Jill Clayton
Information and Privacy Commissioner