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	Association of Professional Engineers and Geoscientists of Alberta (Organization)
Decision number (file number)	P2020-ND-026 (File #013387)
Date notice received by OIPC	June 12, 2019
Date Organization last provided information	January 30, 2020
Date of decision	March 4, 2020
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 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, • email address, • telephone number, • home address, • job title, and • company. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of the information appears to qualify as "business contact information" which is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business email address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation

	to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." Therefore, in my view, PIPA applies in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On June 6, 2019, an employee's email/laptop was accessed without authorization "resulting in a virus containing email being sent from that individual". • Phishing emails were received by staff and individuals in the employee's address book. • The breach was discovered the same day when the emails were recognized as not being "real", and the issue was reported to IT services.
Affected individuals	The Organization reported that the incident affected 6 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately notified external parties. • Quarantined/remediated the employee laptops. • Reviewed options around additional multi-factor authentication. • Will continue regular education program on phishing.
Steps taken to notify individuals of the incident	The Organization reported that affected individuals were notified by email on June 6, 2019.
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: *Access to "address book[”] type information for all but the hacked employee, where any of their personal information would have been on their computer or in their Office 365 files. Advised all 6 individuals that their personal information on their machines may have been compromised and to change necessary information.* In my view, a reasonable person would consider that the contact information at issue, and particularly email address, could be used

	for phishing purposes, increasing vulnerability to identity theft and fraud. This 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 the "Likelihood is low outside of the 6 hacked individuals. Bigger risk of continuation of phishing from the 6 individuals that were affected; they could continue to spread the phish." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the breach was a result of deliberate, malicious access. The Organization did not rule out the possibility that other individuals' personal information was accessed as a result of the six individuals being hacked. Finally, the Organization cannot confirm how much information or for how long the information may have been exposed.

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 information at issue, and particularly email address, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. This is a significant harm. The likelihood of harm resulting from this incident is increased because the breach was a result of deliberate, malicious access. The Organization did not rule out the possibility that other individuals' personal information was accessed as a result of the six individuals being hacked. Finally, the Organization cannot confirm how much information or for how long the information may have been exposed.

I understand the Organization reported that affected individuals were notified by email on June 6, 2019; however, my office has reviewed the notification and found that it did not meet the requirements of the PIPA Regulation.

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) and confirm to my office in writing, within 10 days of the date of this decision, that it has done do. The Organization is also required to confirm that it has considered whether there are any additional affected individuals, and, if there are additional affected individuals, that these individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.

Jill Clayton
Information and Privacy Commissioner