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	Aecon Group Inc. (Organization)
Decision number (file number)	P2017-ND-61 (File #005487)
Date notice received by OIPC	April 28, 2017
Date Organization last provided information	May 23, 2017
Date of decision	May 24, 2017
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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following information was involved in this incident: • name, • health care number, • social insurance number, • emergency contact information, • email addresses, • rate of pay, • apprenticeship information, • union information, and • banking information. 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	• On or about December 8th, 2016, a phishing email was received by an employee of the Organization which went undetected and the employee's credentials were provided to the malicious attacker. • The attacker then accessed the employee's Outlook Web Access and added an email forwarding rule so all emails received by the employee were also forwarded to the malicious attacker's mailbox. This resulted in data leaving the Organization's control and being inadvertently disclosed, including the personal information at issue. • The inadvertent disclosure occurred on two different dates: March 21, 2017 and April 6, 2017.
Affected individuals	The incident affected three (3) employees.
Steps taken to reduce risk of harm to individuals	• Removed the malicious hardware that would redirect the emails to the attacker's mailbox and changed all passwords to the employee's mailbox. • Will remove the ability of employees to implement automatic forwards or redirects of emails and instead will require direct manager and security approval. • Implementing Multi Factor Authentication to all email users to avoid the risk of user credential phishing. • Continue to provide user awareness training to identify and report phishing emails as well as security education and bulletins will be communicated to all email users. • Implementing a Document Management System to protect against confidential information being shared through email. • Continue to provide and promote multiple secure tools and platforms for sharing confidential information. • Continue to reinforce that email is not to be used for transferring confidential information. • Will fully review processes to ensure secure transfer and storage of confidential information.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter sent April 28, 2017.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 did not specifically identify any harm that might result from this incident but reported "Based on the nature of information disclosed, [the Organization] has assessed that there is a real risk of harm." In my view, the identity, employment and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. In addition, email addresses could be used to cause the significant harm of phishing.

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.	As noted above, the Organization reported "Based on the nature of information disclosed, [the Organization] has assessed that there is a real risk of harm." In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and misdirection of email) and 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 as a result of this incident.

The identity, employment and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. In addition, email addresses could be used to cause the significant harm of phishing. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and misdirection of email) and the information has not been recovered.

I require the Organization to notify affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand affected individuals were notified by letter sent April 28, 2017. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner