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	Alberta College of Speech-Language Pathologists & Audiologists (Organization)
Decision number (file number)	P2021-ND-253 (File #021100)
Date notice received by OIPC	March 16, 2021
Date Organization last provided information	December 1, 2021
Date of decision	December 10, 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 individuals 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 operates in Alberta and 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: <u>Group 1</u> (252 individuals): • name, • email address, and • work telephone number. <u>Group 2</u> (6 individuals): Any of the above plus: • mailing address, • professional status, • qualifications (e.g. degrees earned), and • employment information (employer name and time periods). <u>Group 3</u> (2 individuals): Any of the above plus: • credit card number, • date of birth, and/or • passport number.

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On March 12, 2021, several employees of the Organization were the target of an email phishing attack. Two employees provided passwords that would give access to their email accounts. • The Organization reported the breach was discovered when employees found that providing their password did not allow them to login to their email account. • On March 13, 2021, the Organization identified one unknown actor gained access to the email account to one of the two employees' email accounts. • On March 16, 2021, the Organization discovered that there had been unauthorized access to an account, which occurred on March 13, 2021.
Affected individuals	The incident affected approximately 260 individuals.
Steps taken to reduce risk of harm to individuals	• Constrained access to email accounts and systems to Canada only as a further precaution. • Changed IT service providers and enhanced security and privacy from a hardware/software perspective • Enhanced employee training. • Enhanced secure online portal capability so applicants should not be scanning and emailing registration information to staff email accounts
Steps taken to notify individuals of the incident	Affected individuals were notified by email on March 16 and March 17, 2021.
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, *Group 1 - these individuals may be the target of subsequent phishing attacks using their email addresses.* *Group 2 - this information could potentially be used to commit identity theft, although in most cases the information was probably incomplete without the attacker being able to find additional information from other sources.*

	Group 3 - this information could be used to commit identity theft, fraud, negative effects on credit record. In my view, a reasonable person would consider that the contact, identity, employment 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 the affected individuals' vulnerability to identity theft and fraud. These are all 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, *Group 1 - relatively high since this was a phishing attack it seems possible or even likely that the email addresses may be used for subsequent phishing attacks.* *Group 2 - medium to low. The density of this information within the email account was low and finding it through review took diligent searching for several hours, so it would depend on the patience of the searcher. The information available provides an incomplete picture of personal information and so may be of limited value without information from other sources.* *Group 3 - medium to low. Our staff knew what they were looking for and found the credit card information and application information, but it would take a third party some diligent searching to find this information because it isn't a searchable pdf document and would have to first be found, then reviewed manually to find personal information.* 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 employees' email account). The Organization confirmed that there was an unauthorized access to personal information.

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, identity, employment 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 the affected individuals' vulnerability to identity theft and fraud. These are all 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

employees' email account). The Organization confirmed that there was an unauthorized access to personal information.

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).

I understand the Organization notified affected individuals by email on March 16 and March 17, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner