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 School Employee Benefit Plan (Organization)
Decision number (file number)	P2022-ND-045 (File #023178)
Date notice received by OIPC	September 13, 2021
Date Organization last provided information	May 12, 2022
Date of decision	November 8, 2022
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"	"Non-profit organization" is defined in section 56(1) to mean an organization "that is incorporated under the *Societies Act* or the *Agricultural Societies Act* or that is registered under Part 9 of the *Companies Act*." Pursuant to section 56(2), PIPA "does not apply to a non-profit organization or any personal information that is in the custody of or under the control of a non-profit organization", except in the case of personal information that is collected, used or disclosed in connection with any commercial activity. The Organization reported that: 1) It operates as a non-profit organization but is not categorized as one. 2) It is not incorporated under the *Societies Act* or Part 9 of the *Companies Act*. 3) It is a trust created by the Alberta Teacher's Association and The Alberta School Boards Association. In this case, the Organization is not a "non-profit organization" as defined in section 56(1)(b) of PIPA, despite operating on a not for profit basis. Therefore, PIPA applies in this case.

	The Organization 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 the following information: • social insurance number, • address, • date of birth, • personal email address, • salary information, and • benefit and benefit premium information. 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 April 5, 2021, an unauthorized user with an IP address in Nigeria, gained access to an employee's email account. • The unauthorized user accessed the account multiple times between April 5, 2021 and April 8, 2021. • On April 8, 2021, the unauthorized user attempted to initiate a fraudulent wire transfer by using the compromised e-mail address to authorize the wire transfer of an account the Organization believes is controlled by the unauthorized user. • Also on April 8, 2021, the Organization's stakeholders received the fraudulent email posing as an Organization employee. • The Organization's investigation concluded that the unauthorized access to the email account was via web access and that there is no evidence of mailbox synchronization. • In June and July 2021, the Organization began to determine which emails and documents in the email account contained personal information. • The Organization was not able to determine how the unauthorized user accessed the e-mail account. However, there was evidence of multiple failed login attempts prior to the successful login. This suggests a brute-force attack. • The Organization has not been able to determine the extent to which the personal information contained in emails and documents in the email account were accessed by the unauthorized user.
Affected individuals	The incident affected 22,585 individuals whose information was collected in Alberta.

Steps taken to reduce risk of harm to individuals	• Secured compromised email account. • Retained legal counsel to conduct an investigation into the nature and scope of the breach. • Provided identity theft / credit monitoring services to affected individuals. • Updated internal password requirements. • Required all staff to change passwords. • Removed voice call and text as an option for two-factor authentication. • Implemented new cybersecurity training for all staff. • Posted an article on the Organization's intranet that further clarified best practices working with multi-factor authentication. • Updated wire transfer processes to include visual confirmation with approvers and a 3-day lag before processing. • Updated internal processes around processing forms such as banking changes, etc. to include 2nd-level validation when information on form does not match information on file. • Updated Microsoft licensing to include more security features,
Steps taken to notify individuals of the incident	The affected individuals were notified by mail from September 27, 2021 to October 1, 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, *Possible harm that may result from unauthorized access or to the personal information in question may include fraud, identity theft, exposure to phishing campaigns or attempts to obtain further personal information.* *Other than the phishing e-mails to stakeholder, referred to above, the Organization has no evidence at this time that any specific harm has occurred.* In my view, a reasonable person would consider that the contact, identity and employment 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 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	The Organization reported, *The likelihood of harm is low. There is no evidence that the unauthorized user synchronized the compromised e-mail account. Therefore, it is unlikely that the personal information*

between the incident and the possible harm.	*contained in the e-mail account was copied, downloaded or otherwise exfiltrated from the e-mail account.* *However, because the e-mail account was compromised as a result of a malicious act, there remains a risk that the unauthorized user retained some of the personal information contained in the e-mail account, which could be used for malicious purposes including theft, fraud or identity theft.* 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 (email account compromise, fraudulent money transfer request). The unknown third party accessed the employee email account, and used it to send further phishing emails. Further, the unknown third party had access to the Organization's email account for four (4) days.

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 contact, identity and employment 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 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 (email account compromise, fraudulent money transfer request). The unknown third party accessed the employee email account, and used it to send further phishing emails. Further, the unknown third party had access to the Organization's email account for four (4) days.

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 the affected individuals by mail from September 27, 2021 to October 1, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance