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	ABC Head Start Society (Organization)
Decision number (file number)	P2021-ND-311 (File #21682)
Date notice received by OIPC	June 15, 2021
Date Organization last provided information	December 8, 2021
Date of decision	March 4, 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 those 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 is an Edmonton charity and Early Childhood Services (ECS) provider that was founded in 1985. The Organization reported that it is incorporated under Alberta's *Societies Act* and is a "non-profit organization" as defined in section 56(1)(b)(i) of PIPA. 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. Section 56(1)(a)(iv) of PIPA states that a "commercial activity" means "the operation of a private school or an early childhood services program as defined in the *Education Act*." In this case, the Organization operates an early childhood program as defined in the *Education Act*. Therefore, the Organization is engaging in commercial activities. To the extent the personal information at issue in this matter was collected, used and disclosed by the Organization in connection with these activities, PIPA applies.

Section 1(1)(k) of PIPA "personal information"	The incident involved some or all of the following information: <u>Employee:</u> • employment contract, • employee performance evaluation, • insurance contract (date of birth, address, contact numbers, dependent's full name, date of birth, insurance policy number), • banking information, • signature of staff, and • red cross childcare first aid certificate number. <u>Client:</u> • child's full name, • name of parent/guardian, • address, • home/cell telephone number, • email address, • date of birth, • pictures, • Alberta student ID number, • team member names (multiple staff), • health information (weight, height, vision screening, hearing, SLP and other team members' report). 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	• Between May 26, 2021 and May 29, 2021, an intruder gained access to an employee's Microsoft Office 365 account. The Organization later learned the employee had opened email attachments sent by a ransomware email. • On May 29, 2021, a request was received from the employee's compromised account for access to the Organization's Finance SharePoint site. A manager followed up with the employee, who confirmed they had not requested access. • On the same day, Microsoft sent two alerts for unusual volume of file deletion. On May 31, 2021, the Organization's IT coordinator followed up with the employee, who confirmed they had not moved or deleted any files. • On June 2, 2021, the Organization received a ransom demand threatening to release the Organization's data.

Affected individuals	The incident affected 10 individuals (two employees and three families) whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Contacted the police and the Organization's insurance company. • Emailed all staff advising of concerning email received for ransomware and asking them not to open any attachments. • Met with insurance company and cyber investigation firm to further discuss on the details. • Changed staff accounts passwords. • Signed out all staff from all devices. • Looking an enabling multi factor authentication on all accounts. • Revising IT policies and procedures. • Enhancing cyber security training for staff.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on July 21, 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 the possible harms that may occur as a result of the breach are: "Identity Theft, Financial Fraud, Damage to or loss of property, humiliation, Email phishing." I agree with the Organization's assessment. A reasonable person would consider the contact, identity, employment, insurance 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 vulnerability to identity theft and fraud. Health information could be used to cause humiliation or embarrassment. 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, *Our current assessment of the linklihood (sic) of harm being caused to the affected individuals is being assessed by a third party cyber investigation firm and the cyber crimes unit of the Edmonton Police Service. It seems at this time unlikely for further harm to result, but we will update this office if our investigative team communicates further cause for concern.* In my view, a reasonable person would consider 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, ransom demand). In this case, the information at issue was accessed and stolen. It is unclear whether the information has been recovered, and some of

	the affected individuals are part of a vulnerable population (children). Lastly, the information may have been accessible to the intruders for approximately 5 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.

A reasonable person would consider the contact, identity, employment, insurance 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 vulnerability to identity theft and fraud. Health information could be used to cause humiliation or embarrassment. 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, ransom demand). In this case, the information at issue was accessed and stolen. It is unclear whether the information has been recovered, and some of the affected individuals are part of a vulnerable population (children). Lastly, the information may have been accessible to the intruders for approximately 5 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 affected individuals by letter on July 21, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner