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	CUPS Calgary Society (Organization)
Decision number (file number)	P2022-ND-081 (File #023606)
Date notice received by OIPC	November 1, 2021
Date Organization last provided information	June 23, 2022
Date of decision	January 10, 2023
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. Pursuant to section 56(1), "commercial activity" means "the operation of a private school or an early childhood services program as defined by the *Education Act*. In this case, the Organization reported that it is registered under the *Societies Act* and provides an early childhood services program. As a result, PIPA applies.
Section 1(1)(k) of PIPA "personal information"	The incident involved some or all of the following information: • names of children and parent/guardian, • address, • email address, • Alberta Student Number, and

	• Special Education codes. 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 October 21, 2021, a staff member received a phishing email from a trusted email account and was prompted to enter user ID and password. • This resulted in the same phishing link to be sent out to the staff member's entire contact list.
Affected individuals	The incident affected 150 individuals.
Steps taken to reduce risk of harm to individuals	• Notified management, staff and IT teams. • Changed password for user. • Removed rule to auto read emails. • Removed client identifying information from emails. • Working with IT to store information on a secure drive. • Implementing MFA across the Organization.
Steps taken to notify individuals of the incident	Current participants who were affected by the incident were notified by email on October 29, 2021. Affected individuals were also notified by letter/phone on June 23, 2022.
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, *Information could be misued (sic) for identity theft, and further phising (sic) attempts could be made to client emails enclosed within the account.* In my view, a reasonable person would consider that the contact and identity 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	The Organization reported, *Our contracted IT service provider can not say with certainity (sic) the the (sic) personal information contained within the*

or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	*email was not accessed, therefore there is some risk that the information was accessed. They do note that there have not been any events that would indicate her account was used in any capacity.* 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 employee's email account). The lack of reported incidents of identity theft or fraud to date is not a mitigating factor in the likelihood of harm resulting from this incident. Identity theft can happen months and even years after a data breach. As well, the affected individuals are members of a vulnerable population.

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.

Contact and identity 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 (deliberate intrusion into an employee's email account). The lack of reported incidents of identity theft or fraud to date is not a mitigating factor in the likelihood of harm resulting from this incident. Identity theft can happen months and even years after a data breach. As well, the affected individuals are members of a vulnerable population.

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 October 29, 2021, and again by letter/phone on June 23, 2022, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance