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	Children's Wish Foundation of Canada (Organization)
Decision number (file number)	P2019-ND-182 (File #013510)
Date notice received by OIPC	July 16, 2019
Date Organization last provided information	July 16, 2019
Date of decision	December 10, 2019
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 is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	Information involved in the breach may have included: • name, • bank account number, • current annual salary, • termination date, and • employment dispute related documents. The Organization also reported "…the unauthorized third party may have gained access to the affected HR employee's administrator credentials to [the Organization's] payroll provider, who has broad access rights to access and view all employees [sic] records on its payroll processing platform (including income tax statements, payroll stubs and duration of employment …)." This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On May 6, 2019, an HR employee clicked a malicious link included in an email asking her to modify her Office365 password. • The employee immediately alerted the Organization's IT department and changed her password. No abnormal activity was detected by the IT department until May 23, when it noticed the existence of an unauthorized log from Bulgaria dated May 1 and from Turkey dated May 3. • The Organization investigated, contacted Microsoft and retained a forensic cybersecurity firm to determine the root cause of the logs and whether data had been accessed, used or exfiltrated by an unauthorized third party. • On July 15, 2019, the Organization received a report from the cybersecurity firm which concluded that the HR employee laptop had not been compromised and that there was no evidence of unauthorized data access or exfiltration. However, the logs suggest that the unauthorized third party(-ies) had the possibility to create a local copy of the HR employee's mailbox on their own devices.
Affected individuals	The incident affected 122 individuals, including 11 whose personal information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Audited the employee's computer. • Changed the employee's Office365 and payroll processor credentials. • Implementing new security measures, including two-factor authentication. • Developing and deploying an enhanced training program for all employees regarding information security. • Required payroll processor to implement a two-factor authentication on administrator accounts. • Offering all employees prepaid credit monitoring services for 12 months.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on July 16, 2019.

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 harms that could result from the incident included "Risk for fraud, identity theft and phishing attempts". I accept the Organization's assessment. A reasonable person would consider that the financial, employment and tax information potentially at issue could be used to cause the harms of identity theft and fraud. Employment dispute related information could also be used to cause the harms of hurt, humiliation and embarrassment. Credentials could be used to compromise other online accounts. These are 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 the likelihood of harm resulting from this incident is "Unknown". In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing email) and "…the logs suggest that the unauthorized third party(-ies) had the possibility to create a local copy of the HR employee's mailbox on their own devices."

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 financial, employment and tax information potentially at issue could be used to cause the harms of identity theft and fraud. Employment dispute related information could also be used to cause the harms of hurt, humiliation and embarrassment. Credentials could be used to compromise other online accounts. These are significant harms.

The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing email) and "…the logs suggest that the unauthorized third party(-ies) had the possibility to create a local copy of the HR employee's mailbox on their own devices."

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 affected individuals were notified by email on July 16, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner