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	Christian Labour Association of Canada (Organization)
Decision number (file number)	P2021-ND-229 (File #018429)
Date notice received by OIPC	November 30, 2020
Date Organization last provided information	November 30, 2020
Date of decision	November 12, 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 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 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 incident involved all or some of the following information: • name, • address, • social insurance number, • date of birth, • banking information, • tax information, and • employee ID number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On October 15, 2020, the Organization was subject to a ransomware attack. The Organization reports that servers were encrypted and records were likely exfiltrated. • The Organization was unable to determine how the attacker gained access to their environment.
Affected individuals	The incident affected 620 of individuals, including 100 whose information was collected in Alberta.

Steps taken to reduce risk of harm to individuals	• Engaged a cyber security firm.
	• Notified police.
	• Implemented cybersecurity training with a focus on phishing.
	• Implemented or upgraded a number of technical safeguards including:
	  ○ mandatory two-factor authentication for web based access and network,
	  ○ network scanning of all outbound activity,
	  ○ firewall based website filtering,
	  ○ secured certain organization devices and provided only the required account and network access,
	  ○ updating all computer assets,
	  ○ centralized log monitoring and alerting for suspicious behaviour, and
	  ○ operational checks to maintain security compliance.

Steps taken to notify individuals of the incident	Affected individuals were notified by email and letter on November 27, 2020.
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 breach could result in the possible harms of "identity theft, [and] fraud." I agree with the Organization's assessment. A reasonable person would consider the identity, contact, employment, tax and banking information at issue could be used to cause the significant harms of identity theft and fraud.
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: *In our view, the risk of harm is low because while the information was sensitive, there were no artificates [sic] indicating the attacker navigated through folders and files to prioritized [sic] certain information. We have no conclusive evidence that the sensitive personal information on this server was in fact accessed and/or exfiltrated, we*

	only have Firewall logs that show outbound traffic to an inappropriate IP address. Checks of the attacker's web site and dark web searches did not show any data was posted. 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 a third party (deliberate intrusion, deployment of ransomware). Despite having no "conclusive evidence" that personal information was accessed or exfiltrated, the Organization did not rule out the possibility.

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 identity, contact, employment, tax and banking information at issue could be used to cause the significant harms of identity theft and fraud.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (deliberate intrusion, deployment of ransomware). Despite having no "conclusive evidence" that personal information was accessed or exfiltrated, the Organization did not rule out the possibility.

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 and letter on November 27, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner