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	La Leche League International (Organization)
Decision number (file number)	P2021-ND-230 (File #019443)
Date notice received by OIPC	February 9, 2020
Date Organization last provided information	February 9, 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's head office is on Raleigh, NC, USA. The Organization 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: • first and last name, • address, • email address, • telephone number, • accreditation date, • lifetime giving total amount, • first gift amount and date, • most recent gift amount and date, and • largest gift amount and date. 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	• In May 2020, the Organization's cloud-based software and data hosting solutions provider (Blackbaud) was targeted by a ransomware attack during which threat actors managed to remove a subset of data from Blackbaud's self-hosted environment, which included data being processed by Blackbaud for the Organization. • On or around July 16, 2020, the Organization received a notification from Blackbaud informing it of the incident. • The cybercriminal encrypted Blackbaud's data and demanded a ransom payment.
Affected individuals	The incident affected 188,000 individuals, including 649 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Notified its constituents of the incident via email newsletters and a notice on its website. • Set up an email account for individuals that may have questions and updated its website with information on the incident. • Sought assurances from Blackbaud to confirm that the threat actors did not access credit card information, bank account information, or social security numbers. Moreover, Blackbaud assured the Organization that it is confident that the files affected by the incident have been destroyed by the threat actors. • Retained privacy counsel to further investigate the nature and scope of the incident and confirm the impacts on constituents. • Liaising with Blackbaud to discuss the handling of the incident and understands that Blackbaud has also implemented several changes that will reduce the risk of a similar event occurring in the future. • Updating its privacy policy.
Steps taken to notify individuals of the incident	Affected individuals were notified by newsletters sent on July 22, 2020 and July 27, 2020, and by letter on January 22, 2021.

<table>
<tr><th colspan="2">REAL RISK OF SIGNIFICANT HARM ANALYSIS</th></tr>
<tr><td>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.</td><td>The Organization reported,

The possible consequences might include the loss of confidentiality of personal data and phishing.

In my view, a reasonable person would consider that contact and donor information could be used to cause the significant 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.</td></tr>
<tr><td>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.</td><td>The Organization reported the likelihood of significant harm will result is “unlikely”, and that it “... has no indication that any personal information has been subject to actual or attempted misuse in relation to this Incident.”

In my view, a reasonable person would consider the likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to a deliberate unauthorized intrusion by a cybercriminal. The Organization reported that the cybercriminal both accessed and stole the personal information at issue. The Organization can only assume that cybercriminal did not or will not misuse, disseminate or otherwise make public the personal information at issue. The Organization reported the personal information may have been exposed for approximately three and a half (3 ½) months.</td></tr>
<tr><th colspan="2">DECISION UNDER SECTION 37.1(1) OF PIPA</th></tr>
<tr><td colspan="2">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 contact and donor information could be used to cause the significant 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 significant harm resulting from this incident is increased because the personal information was compromised due to a deliberate unauthorized intrusion by a cybercriminal. The Organization reported that the cybercriminal both accessed and stole the personal information at issue. The Organization can only assume that cybercriminal did not or will not misuse, disseminate or otherwise make public the personal information at issue. The Organization reported the personal information may have been exposed for approximately three and a half (3 ½) months.</td></tr>
</table>

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 newsletters sent on July 22, 2020 and July 27, 2020, and by letter on January 22, 2021. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner