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	Center Street Church (Organization)
Decision number (file number)	P2021-ND-183 (File #017791)
Date notice received by OIPC	October 19, 2020
Date Organization last provided information	October 19, 2020
Date of decision	October 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 on a not for profit basis. 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. "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*." In this case, the Organization is established under Federal legislation and does not qualify as a "non-profit organization" as defined in section 56(1)(b) of PIPA, despite operating on a not for profit basis. Therefore, PIPA applies in this case. 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: <u>General personal information</u> • name, • contact information (email, mailing address, telephone number), • gender, • date of birth, • photo, and • information about family members (children and spouses). <u>Donor-related information</u> • name, • contact information, • donation amounts, • dates, • scanned banking information in limited cases (i.e. cheques or hand-written credit card numbers. Please note that bank account or credit card numbers from online giving was not involved in this incident). <u>Current or past employees, staff and human resources</u> • name, • contact information, • date of birth, • social insurance number, • employment details, and • payroll (including bank account information) and benefits information. <u>Operational or ministry information</u> • name, • contact information, • library borrowing history, • children/youth ministry information (such as attendance records), • emails, • information associated with specific mission trips (scans of passports and Alberta Health Care numbers, and volunteer information such as reference checks, skills information). 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 June 13, 2020, the Organization began to experience system outages. An investigation revealed that two servers had been encrypted by ransomware. • The Organization did not pay the ransom and reported the incident to the authorities. • The Organization restored the servers from backup copies. • The Organization reported that it does not have any evidence or direct indication that sensitive data was copied (exfiltrated) in addition to being encrypted, but said it cannot rule out the copying of data. • The Organization also reported that while there was encryption of data and a request for ransom, its investigation determined that there is no evidence that any information was accessed in this incident.
Affected individuals	The incident affected 87,577 individuals, of which 84,513 were individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately took exposed machines offline, restricted administrative accounts, changed administrative passwords, reviewed firewall logs. • Implemented additional security measures. • Reported the incident to police services. • Hired a cybersecurity specialist to manage the recovery, mitigation, and response to the incident. • Conducted a risk analysis to evaluate what additional recovery activities were necessary. • Developed and executed a communications plan to manage communication and response activities. • Upgraded to remove old versions of software on networks. • Improved monitoring and auditing of computer systems. • Created a tiered incident response team trained to answer questions about the incident. • Held "open houses" to talk with affected individuals and answer any questions, provided guidance to individuals affected by the incident, and offered credit monitoring services to parties whose banking information was present on the affected systems. • Updated IT security policies and procedures. • Providing security and privacy training to staff. • Considering a future organization-wide privacy gap assessment to identify risks in the management of personal information.

	• Evaluating personal information collected and maintained moving into the future. • Migrating data into a new customer relationship management software system that ensures appropriate security controls.
Steps taken to notify individuals of the incident	The Organization reported that "Notification will be provided in various forms including email, letter, in a posting on the … website, and announced during regular church services" and that "Notification will be complete by October 31, 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 possible harms that could occur as a result of this incident include identity theft, fraud, and damage to reputation. Given that email addresses were possibly at risk, future phishing campaigns or attempts to solicit monetary donations could possibly occur.* I agree with the Organization's assessment. A reasonable person would consider the contact, identity, donation, employment and religious information at issue could be used to cause the significant harms of identity theft, fraud, and damage to reputation. Email addressed could be used for phishing, increasing vulnerability to 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: *We assess the likelihood that harm will result as moderate. While the ransomware attack was done by an unknown individual with malicious intent, it appears that person was looking to profit from the attack and not to steal any personal information. Accordingly, our assessment as to the moderate risk of harm is presented below:* *- the systems affected were shut down within 24 hours of the incident occurring.* *- the investigation found that there was no evidence of any data exfiltration (data theft). That said, we cannot confirm with certainty that personal information was not accessed or copied.* *With all of this said, we are unable to confirm with 100% certainty that data on the impacted systems was not accessed or copied in addition to being encrypted. The ransomers did not threaten to release any information if the ransom was not paid, nor did investigators discover any evidence of exfiltration or*

	data access. However, since data access cannot be completely ruled out, out of an abundance of caution, we are reporting the breach and we have created a substantial internal response to ensure we respond to questions or circumstances that may arise. I agree with the Organization's assessment. 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). Although the Organization said there was no evidence discovered concerning exfiltration of data, it cannot be completely ruled out.

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, donation, employment and religious information at issue could be used to cause the significant harms of identity theft, fraud, and damage to reputation. Email addressed could be used for phishing, increasing vulnerability to 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 an unknown third party (deliberate intrusion, ransom demand). Although the Organization said there was no evidence discovered concerning exfiltration of data, it cannot be completely ruled out.

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 reported that "Notification will be provided in various forms including email, letter, in a posting on the … website, and announced during regular church services" and that "Notification will be complete by October 31, 2020". **I require the Organization to confirm to my office, in writing, within ten (10) days of the date of this decision, that affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.**

Jill Clayton
Information and Privacy Commissioner