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	Ransomed Heart Ministries (Organization)
Decision number (file number)	P2017-ND-56 (File #001368)
Date notice received by OIPC	August 4, 2015
Date Organization last provided information	April 3, 2017
Date of decision	May 15, 2017
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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is Colorado-based and operates on a not for profit basis. However, it is not a "non-profit organization" as defined in section 56(1)(b) of PIPA. The Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • billing information, • mailing address, • email address, • debit card information, and • credit card information (including security code and expiration date). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from residents of Alberta via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On June 8, 2015, the Organization's web hosting company detected possible malicious activity involving its website. • Within hours of discovery, the hosting company secured the website. • The incident was reported to the Organization on June 15, 2015. • The Organization reported the information may have been exposed for six weeks and there was evidence of malicious code.
Affected individuals	A total of 1,384 individuals were affected by the incident, including 8 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Secured the website. • Engaged a forensic IT firm to assist in the investigation. • Notified the Privacy Officer and the United States Secret Service. • Reported the incident to the Office of the Information and Privacy Commissioner of Alberta.
Steps taken to notify individuals of the incident	Affected individuals were notified by email sent on July 30, 2015.
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 that "Customers may experience fraudulent charges on their credit card or debit card." In my view, the financial information at issue (including card security code and expiration date) could be used to cause identity theft and fraud. Email addresses could be used to gain unauthorized access to other internet accounts and could be used for phishing purposes. 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 did not specifically assess the likelihood of harm resulting from this incident but reported "lt is possible that fraudulent charges could result." In my view, 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 and installation of malware). The information was possibly exposed for six weeks, and has not been recovered.
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.	

The financial information at issue (including card security code and expiration date) could be used to cause identity theft and fraud. Email addresses could be used to gain unauthorized access to other internet accounts and could be used for phishing purposes. These are 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 and installation of malware). The information was possibly exposed for six weeks, and has not been recovered.

I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals in an email dated July 30, 2015, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner