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	Heart and Stroke Foundation of Canada (Organization)
Decision number (file number)	P2019-ND-202 (File #012995)
Date notice received by OIPC	April 10, 2019
Date Organization last provided information	April 10, 2019
Date of decision	December 16, 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"	The Organization reported "Principally, the incident involved the use of email addresses associated with the user's email account". 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 February 4, 2019, it was brought to a user's attention that the user's email account had been used to send emails that appeared to be suspicious. • Internal IT and outside consultants determined that someone unknown had accessed the user's email account and used it to send emails with a fraudulent purpose. No evidence of data exfiltration or any other access to the Organization's resources were found.

	• The investigation revealed a number of suspicious logins to other of the organization's email inboxes but there was no evidence that these inboxes were used for sending similar messages.
Affected individuals	The incident affected approximately 4,657 individuals, including approximately 60 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Locked down the user's account and investigated. • Reviewing and considering next steps, including implementing multi-factor authentication for all VPN connections, increasing company-wide security training and evaluating external cloud infrastructures.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on March 26, 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 "These email addresses can be used for fraud, and the unknown perpetrator attempted to do so". In my view, a reasonable person would consider that the email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. 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 "Nobody has reported having been duped by this fraud attempt, but there is a risk of harm arising". 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 (deliberate action and phishing emails sent). The fact there have been no reported incidents of successful fraud to date does not mitigate against future harm as identity theft and fraud can occur months or even years after an incident.
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 email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action and phishing emails sent). The fact there have been no reported incidents of successful fraud to date does not mitigate against future harm as identity theft and fraud can occur months or even years after an incident.

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 March 26, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner