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)	P2016-ND-13 (File #000202)
Date notice received by OIPC	September 9, 2014
Date Organization last provided information	January 14, 2016
Date of decision	March 14, 2016
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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is federally incorporated as a not-for-profit corporation. Section 56(3) limits the application of PIPA to personal information collected, used or disclosed by a "non-profit organization" in connection with a commercial activity. Although it operates on a not-for-profit basis, the Organization is not a "non-profit organization," as defined by section 56(1)(b)(i) of PIPA. I have jurisdiction because 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 the following information: • name; • email address.

	This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On September 5, 2014, the Organization discovered that names and email addresses of individuals were inadvertently stored on an unsecure server by the Organization's service provider. The server was connected to the internet. • The Organization reported there was no evidence that the information was accessed by unauthorized individuals. • The incident was caused by human error.
Affected individuals	There were 918 affected individuals in Alberta.
Steps taken to reduce risk of harm to individuals	Upon discovering the breach, the information was moved to a secure server.
Steps taken to notify individuals of the incident	Affected individuals were notified via email on September 9, 2014.
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 "it had made the determination that a reasonable person would not consider that there exists a real risk of significant harm" as a result of this breach, and noted only very limited personal information was involved (names and email addresses). In my view, the personal information involved could be used to cause the harms of phishing and spam emails. 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 that the incident was caused by human error, rather than through a security breach, and was "immediately rectified". The Organization has no evidence that any of the affected individuals have been impacted in any way. Despite the lack of malicious intent, in my view there is a real risk of harm resulting from this breach. The Organization did not confirm the length of time the information was exposed, and did not provide evidence that the information was not accessed during this time.

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 personal information involved could be used for social engineering attacks such as targeted phishing and spam emails. These are significant harms. The Organization did not confirm the length of time the information was exposed, and did not provide evidence that the information was not accessed during this time. I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals on September 9, 2014. The Organization is therefore not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner