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	Prostate Cancer Canada (Organization)
Decision number (file number)	P2015-ND-28 (File #000041)
Date notice received by OIPC	December 9, 2014
Date Organization last provided information	March 14, 2015
Date of decision	May 15, 2015
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"	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 all or some of the following information about the individuals: • email addresses; • first (and in some cases) last names associated with the email addresses; • city, province and/or postal codes associated with the email addresses in some cases. 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 November 24, 2014 a third party hacker accessed a microsite operated by the Organization. • The breach was discovered by an Organization member who noticed a graphic and message posted on the site by the hacker. • The Organization contacted the hosting vendor and the vulnerability was fixed within five hours. • The breach involved the personal information of individuals who had posted pictures on the website.
Affected individuals	The incident involved 1,275 affected individuals, including 117 Albertans.
Steps taken to reduce risk of harm to individuals	• The website vendor immediately removed the graphic and message from the website. • The vulnerability was immediately fixed.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on December 8, 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 recognized that the affected individuals may be at risk for targeted advertising, spam, or fraud through phishing and identity theft. In my view, the personal information disclosed is of low to moderate sensitivity. However, it could be used to cause the harm of fraud through phishing and identity theft. 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 submitted that there was a low risk of significant harm as the email addresses, city/province /postal codes and last names were of a general nature (e.g., not specific street addresses), contained no passwords, and were not linked to any other information on the site. However, the Organization recognized that the breach could allow a third party to connect photos with first and last names, as well as email addresses. In my view, although the personal information at issue is of low to moderate sensitivity, the likelihood of harm is increased because the information was accessed by a hacker with malicious intent. Further, the number of affected individuals increases the risk of phishing.

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. Although the personal information at issue is of low to moderate sensitivity, the likelihood of harm is increased because the information was accessed by a hacker with malicious intent. Further, the number of affected individuals increases the risk of phishing. These factors contributed significantly to my decision. 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 the affected individuals by email and therefore is not required to do so again.

Jill Clayton
Information and Privacy Commissioner