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	RateMyProfessors.com LLC (Organization)
Decision number (file number)	P2016-ND-22 (File #002107)
Date notice received by OIPC	January 8, 2016
Date Organization last provided information	February 25, 2016
Date of decision	March 15, 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 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 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: • email address, • password, and • date of registration. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	Hackers gained unauthorised access to a decommissioned version of the Organization's website by exploiting a vulnerability in an internet facing application within the site.
Affected individuals	A total of 33,000 individuals in Canada were affected. The Organization is unable to determine how many Albertans were affected because the website does not collect location information from its users.
Steps taken to reduce risk of harm to individuals	• The security vulnerability has been turned off and access to it has been blocked. • Encryption is required for stored passwords. • Review of decommissioning procedures is underway. • Password change was required for all registered users.
Steps taken to notify individuals of the incident	Notification sent by email to affected individuals on January 6, 2016.
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 did not specifically identify the type of harm that might result from this incident, but noted that "there is no evidence at this time that these credentials were used in an unauthorized fashion" and that the website does not collect sensitive identity information. I agree with the Organization that the information involved does not include sensitive identity information such as date of birth, or social insurance number. However, the information does include user emails and passwords, which could be used to gain unauthorized access to other online accounts, and could result in phishing and/or 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 submitted that the risk of harm is "small" and it is continuing to monitor the website and overall account activity for any anomalies. In my view, the likelihood that harm will result from this incident is increased because the information at issue was obtained by hackers, indicating malicious intent, and the information 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 personal information at issue includes user emails and passwords, which could be used to gain unauthorized access to other online accounts, and could result in the significant harms of phishing and/or fraud. The risk of harm is increased because the information at issue was obtained by hackers, indicating malicious intent, and has not been recovered. 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 via email on January 6, 2016 in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner