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	Running Room Canada (Organization)
Decision number (file number)	P2020-ND-086 (File #013863)
Date notice received by OIPC	November 15, 2019
Date Organization last provided information	November 20, 2019
Date of decision	July 28, 2020
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 an "organization" as defined in section 1(1)(i) of PIPA. The Organization is an Alberta based company with customers across the country.
Section 1(1)(k) of PIPA "personal information"	The incident involved some or all of the following information: • name, • email address, and • hashed password. This information is about identifiable individuals and is "personal Information" as defined in section 1(1) (k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On November 14, 2019, the Organization's web security team identified an SQL injection and confirmed unauthorized access to its website database containing user profile information. • The compromised information "…did not involve sensitive personal information like government-issued IDs (like Social Insurance numbers and driver's license numbers) or payment cards, bank account, or other financial information".

Affected individuals	The Organization reported it "…found 180,876 hits from attacker's IP in the logs. No way to know how many of those returned email addresses so the maximum would be 180,876 emails + encrypted passwords. We are working on this now and will soon have a list of all exposed email addresses [sic]."
Steps taken to reduce risk of harm to individuals	• Detected the unauthorized access and blocked it immediately. • Made additional changes to the site to prevent the incident from reoccurring. • Blocked the injection and removed the page (it is no longer in use).
Steps taken to notify individuals of the incident	The Organization posted a notice on its website on November 15, 2019, but did not notify affected individuals directly.
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: *We do not consider that there exists a real risk of significant harm to an individual as a result of unauthorized access…this incident did not involve sensitive personal information like government-issued IDs (like Social Insurance numbers and driver's license numbers) or payment cards, bank account, or other financial information.* *[The Organization] has always cryptographically protected passwords using a technique known by security experts as "salted hashing." The benefit of hashing passwords is that we never need to store the passwords in plain text.* In my view, a reasonable person would consider it unlikely that hashed and salted passwords could be used to cause significant harm. Email addresses, however, could be used for phishing, increasing affected individuals' 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 that there is a "very low likelihood of harm." In my view, a reasonable person would consider 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 a significant number of accounts were affected.

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 it unlikely that hashed and salted passwords could be used to cause significant harm. Email addresses, however, could be used for phishing, increasing affected individuals' vulnerability to identity theft and fraud. 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 a significant number of accounts were affected. **I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act* Regulation (Regulation) and require the Organization to confirm to my Office in writing, within ten (10) days of the date of this decision, that affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation. If the Organization believes direct notice is unreasonable in the circumstances, it may make a submission to me before the 10 days expire, giving its reasons why direct notice is unreasonable.**

Jill Clayton
Information and Privacy Commissioner