



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Running Room Canada Inc. (Organization)
Decision number (file number)	P2022-ND-004 (File #028704)
Date notice received by OIPC	January 20, 2023
Date Organization last provided information	January 27, 2023
Date of decision	February 1, 2023
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 <i>Personal Information Protection Act</i> (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”	<p>The incident involved some or all of the following information:</p> <ul style="list-style-type: none">• email address,• phone number,• address,• credit card number,• expiry date, and• CVV code. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. To the extent the information at issue was collected in Alberta, PIPA applies.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• On November 19, 2022, an unauthorized group obtained access to the Organization’s Canadian online shop checkout between the dates of November 19, 2022 to January 18, 2023.

	<ul style="list-style-type: none"> The Organization is working with law enforcement who notified the Organization that a USA agency identified an active infection on ca.shop.runningroom.com.
Affected individuals	The incident affected 14,589 including 1,877 residents of Alberta.
Steps taken to reduce risk of harm to individuals	<p>Steps taken include some or all of the following:</p> <ul style="list-style-type: none"> Removed the vulnerability immediately upon becoming aware of the unauthorized access. Working with law enforcement. Notified data protection authorities. Implemented enhanced security measures.
Steps taken to notify individuals of the incident	<p>Affected individuals were notified by email on January 23, 2023</p> <p>The Organization also posted a notice on its website.</p>
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>Harm</p> <p>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.</p>	<p>The Organization reported,</p> <p><i>Sale of the user's credit card resulting in fraudulent use of the cards. Phishing and social engineering are also possible results of the information gathered.</i></p> <p>In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms.</p>
<p>Real Risk</p> <p>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.</p>	<p>The Organization reported,</p> <p><i>The likelihood is high, it is believed the intent of acquiring the information was for resale for fraudulent transactions and testing vulnerabilities. Individuals affected will receive a direct notification with the appropriate information as outlined in PIPA regulation 19.1.</i></p> <p>I agree with the Organization’s assessment. 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). Further, the information may have been exposed for approximately 2 months.</p>

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 contact and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all 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). Further, the information may have been exposed for approximately 2 months

I require the Organization to notify the affected individuals whose information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by email on January 23, 2023, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance