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	iHerb Inc. (Organization)
Decision number (file number)	P2021-ND-324 (File #020733)
Date notice received by OIPC	April 23, 2021
Date Organization last provided information	April 23, 2021
Date of decision	March 9, 2022
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 whose personal information was collected in Alberta, pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is a U.S. e-commerce company that sells vitamins, supplements and other related products to consumers. The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • telephone number, • email address, • postal code, and • the last four digits and expiration date of payment card if the customer stored a card in the account. 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 via the Organization's website and/or application. In its notification to affected individuals, the Organization stated, "If you reside outside of the U.S. and you stored a national identification number or passport number in your … account, this

	information also may have been accessible to the unauthorized party."
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• The Organization experienced a breach that resulted in compromised user accounts. • The Organization's notice to affected individuals said that "…beginning in mid-October 2020, an unauthorized party used the login credentials (i.e., email and password) of certain of our customers to access their … accounts. Based on our investigation, the compromised credentials appear to have been taken from third parties independent of [the Organization] and were not obtained as a result of a compromise of our systems. The unauthorized party may have used these stolen credentials to purchase… products with your existing Rewards credits or your stored payment card." • The Organization reported that the unauthorized party used the login credentials of 3 customers in Alberta to access their online accounts between January 14, 2021 and February 1, 2021. • Of the three affected Alberta customers, the unauthorized parties used two customer accounts to engage in activity on the Organization's website that fraudulently generated new Rewards credits that were added to the relevant accounts. • These new Rewards credits were used to purchase the Organization's products on only one customer account.
Affected individuals	The incident affected 3 Alberta customers.
Steps taken to reduce risk of harm to individuals	• Retained a data security expert to conduct a forensic investigation. • Took actions to secure customer accounts. • Locked affected accounts, required a password reset, and working with affected customers to restore legitimate email addresses. • Continuing to monitor for suspicious activity. • Taking a number of steps to help prevent further account takeover activity by the unauthorized parties and abuse of the Rewards program. • Enhancing measures for detecting and blocking automated activity on the Organization's website. • Working to further expand monitoring and anomaly detection capabilities, with a particular focus on customer login activity.

Steps taken to notify individuals of the incident	Affected individuals were notified of the incident on April 21, 2021.
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 "…believes that the primary motivation for this credential stuffing activity was to commit fraud against [the Organization] (rather than against customers) by abusing [the Organization's] Rewards program." The Organization's notification to affected individuals said: *We are alerting you about this issue so you can take steps to help protect yourself, such as the following:* • *If you detect an unauthorized purchase of [the Organization's] products using your payment card, please contact your payment card company or financial institution. …* • *Change your credentials for any other online service if you used a username and password that are the same as or similar to those used for your … account.* • *Monitor your …account for suspicious activity. If you believe that fraudulent activity has occurred on your account, please contact [the Organization] at….* In my view, a reasonable person would consider the contact information, combined with email address, could be used for phishing or impersonation, increasing vulnerability to identity theft and fraud. Confirmed valid credentials could be used to compromise online accounts. 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 it "…believes that the primary motivation for this credential stuffing activity was to commit fraud against [the Organization] (rather than against customers) by abusing [the Organization's] Rewards program." Further, it "…does not believe that these customers experienced fraud with respect to Rewards credits that they had legitimately earned or any other type of financial loss." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the incident appears to be the result of malicious action (deliberate, credential stuffing, fraudulent activity). The Organization can only speculate as to the motives of the perpetrators. It appears the information may have been exposed for some time before the Organization became aware of the breach.

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 the contact information, combined with email address, could be used for phishing or impersonation, increasing vulnerability to identity theft and fraud. Confirmed valid credentials could be used to compromise online accounts. These are significant harms. The likelihood of harm resulting from this incident is increased because the incident appears to be the result of malicious action (deliberate, credential stuffing, fraudulent activity). The Organization can only speculate as to the motives of the perpetrators. It appears the information may have been exposed for some time before the Organization became aware of the breach. I require the Organization to notify the affected individuals whose personal 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 on April 21, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner