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	rewardStyle Inc. (Organization)
Decision number (file number)	P2021-ND-188 (File #017671)
Date notice received by OIPC	October 6, 2020
Date Organization last provided information	October 6, 2020
Date of decision	October 14, 2021
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 *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.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • address, • telephone number, • email address, • hashed and salted password, • website /blog name, • URLs, and • social media usernames. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On March 8, 2020, the Organization identified unusual activity on its websites rewardstyle.com and about.rewardstyle.com.

	• The Organization investigated and found that an attacker had the ability to take over and redirect the website URLs but the investigation was inconclusive with respect to any access to the Organization's information. • The Organization reported that there was no unauthorized activity after March 8, 2020 • On June 1, 2020, the Organization discovered that unauthorized individual(s) may have acquired certain personal data stored in its databases and had taken steps to make the data available for download to other third parties. • On July 17, 2020, the Organization was able to obtain a copy of the data tables to verify that the data belonged to the Organization. • The Organization believes that the information may have been taken on or about February 12, 2020.
Affected individuals	The incident affected 3,315 individuals, including 732 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Forces a reset of passwords. • Reported the incident to U.S. law enforcement. • Implemented several technical safeguards.
Steps taken to notify individuals of the incident	The Organization provided indirect notification via a blog post on its website in June 2020. Direct notification to affected individuals was completed on October 5, 2020.
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, *It is theoretically possible that the information could be used for phishing of individuals or credential stuffing in the event users have reused passwords, although there is no evidence to date.* In my view, a reasonable person would consider that the contact and credential information, along with email addresses, could be used to compromise other online accounts and for phishing, increasing the 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	The Organization reported, *Although there is no evidence of actual harm, the information was acquired by malicious actors who traded the information on the dark web.*

between the incident and the possible 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 the information was traded on the dark web.

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 that the contact and credential information, along with email addresses, could be used to compromise other online accounts and for phishing, increasing the 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 the information was traded on the dark web.

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

I understand the Organization completed notifying affected individuals by letter on October 5, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner