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	You Can Trade Inc., a subsidiary of TradeStation Group Inc. (Organization)
Decision number (file number)	P2020-ND-158 (File #016162)
Date notice received by OIPC	June 11, 2020
Date Organization last provided information	June 11, 2020
Date of decision	November 20, 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 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 an on-line education service company based in the USA, and 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: • first and last name, • username, • password (salted and hashed), • email address, • telephone number, • billing address, and • credit card data (credit card type, last four digits of the credit card account number and credit card expiry date). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On May 28, 2020, the Organization discovered that customer personal data had been accessed by one or more unauthorized persons in February. • The Organization discovered that two domains were hosting a replica of the Organization's website; one in Iran, and the other in India. • A recently hired developer made an unauthorized back up copy of the Organization's database and website, and imported the data to an unauthorized server. The system was unprotected, with ports open to the internet. • The Organization's investigation indicated that the back up data was accessed by an IP address originating in China. • The Organization reported that it relocated its systems from the hosting facility where the data was copied by the developer into Amazon Web Services, to reduce the likelihood of reoccurrence.
Affected individuals	The incident affected thirty-six (36) Canadians, including 7 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Has a comprehensive incident response plan that facilitates the detection, review, and containment of an incident. • Implemented additional security measures. • Identified two domains that accessed the data and were mimicking the appearance of its website and promptly acted and shut down both domains.
Steps taken to notify individuals of the incident	Affected individuals were notified by email June 10, 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 "In the unlikely event that passwords are able to be unencrypted, (i) the breach could result in unauthorized access to a customer's … account (which would provide access to investment educational content such as videos or webinars) and (ii) it is possible that there could be other consequences from the breach if one or more data subjects use the same username and password that are used for [the Organization] to log into accounts that they maintain with other companies". In my view, a reasonable person would consider the contact and profile information (customer of Organization, username) in conjunction with email address could be used for the purposes of phishing, increasing 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, *Given the types of personal data that may be affected (particularly given that passwords are salted and hashed and limited credit card data was accessed (only the last four digits of credit card numbers were accessed)), we believe that there is no real risk of significant harm to individuals* In its notice to affected individuals, the Organization said, *As a precautionary measure, we recommend that you remain vigilant and do not click on any emails that you may receive that may seem suspicious and/or may contain any links or language with the above referenced domains (shayand.com or youcantrade.urtestsite.com)...Fraudulent activity or any suspected incidence of identity theft may be reported to proper law enforcement authorities, including your local police force and the Canadian Anti-Fraud Centre* In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unauthorized person(s). The Organization reported that the personal information was already accessed for fraudulent or unauthorized purposes. Further, the information may have been exposed for approximately three (3) months.

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 and profile information (customer of Organization, username) in conjunction with email address could be used for the purposes of phishing, increasing 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 unauthorized person(s). The Organization reported that the personal information was already accessed for fraudulent or unauthorized purposes. Further, the information may have been exposed for approximately three (3) months.

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 by email on June 10, 2002 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner