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	StockX LLC (Organization)
Decision number (file number)	P2020-ND-024 (File #013701)
Date notice received by OIPC	September 11, 2019
Date Organization last provided information	September 11, 2019
Date of decision	March 3, 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 "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, • email address, • physical address, • username, • hashed password, and • purchase history. 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.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On July 26, 2019, the Organization was alerted to suspicious activity potentially involving customer data.

	• The Organization investigated and engaged third party experts to assist. • The investigation found that an unknown third party had been able to gain unauthorized access to certain customer data from the Organization's cloud environment on or around May 14, 2019.
Affected individuals	The incident affected 6.8 million customers, including 120,000 Canadians (10,901 of whom are residents of Alberta).
Steps taken to reduce risk of harm to individuals	• Updated systems, which upgraded the encryption of customer passwords. • Reset all customer passwords and emailed customers alerting them about the system update and the password reset. • Locked down the Organization's Amazon Web Services (AWS) perimeter. • Emailed all customers to alert them of the incident and to provide them with information regarding steps the Organization is taking and what steps customers can take to protect themselves. • Obtained 12 months of free fraud detection services for its customers. • Established a third party call centre to field questions. • Notified law enforcement agencies and data protection authorities.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on August 3, 2019 and August 8, 2019.
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 "Based on the nature of the incident, it is possible that potential harm to customers could include the misuse of the usernames and hashed passwords acquired by the unknown third-party hacker." In my view, a reasonable person would consider that the contact and profile information (purchase history, relationship to the Organization), as well as partial credentials (username, hashed password), could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.

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 "In light of the nature of the personal information affected by the breach (i.e. low sensitivity information that does not include any financial or payment information), [the Organization] is of the view that the breach does not present any real risk of significant harm to any individual". The Organization also said that it "…has no indication that any actual harm to data subjects has yet occurred as a result of the incident". In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the incident resulted from malicious action (deliberate attack) and the breach was not discovered for almost 3 months. The fact there are not reports of actual harm to date does not mitigate against future harm as identity theft and fraud can occur months or even years after an incident.

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 profile information (purchase history, relationship to the Organization), as well as partial credentials (username, hashed password), could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.

The likelihood of harm resulting from this incident is increased because the incident resulted from malicious action (deliberate attack) and the breach was not discovered for almost 3 months. The fact there are not reports of actual harm to date does not mitigate against future harm as identity theft and fraud can occur months or even years after an incident.

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 August 3, 2019 and August 8, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner