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	Victoria's Secret Stores Brand Management (the Organization)
Decision number (file number)	P2021-ND-194 (File #0018648)
Date notice received by OIPC	December 9, 2020
Date Organization last provided information	December 9, 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 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 Organization reported the incident involved some or all of the following information: • name, • email address, • postal address (if entered), • birth day and month (not year), • last four digits of payment card (if provided), and • telephone number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization experienced a credential-stuffing attack which took place over an approximately four-hour period on November 9, 2020. • As a result, an unauthorized individual gained access to personal information in certain of the Organization's online accounts. • The attack was detected and later blocked by the Organization while it was still in progress. • The Organization reported that, based on its investigation, the incident resulted from the apparent reuse of legitimate, recycled credentials (usernames and passwords) that may have been obtained in third-party hacking incidents.
Affected individuals	The Organization reported approximately 16 individuals whose information was collected in Alberta were affected.
Steps taken to reduce risk of harm to individuals	• Took steps to secure the accounts and determine the nature of the cyber attack. • Asked customers to change their current passwords and create new ones, and to monitor their online account for suspicious activity. • Maintains, and continuously enhances, a documented information security program with numerous controls to detect and mitigate cyber attacks.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on December 9, 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 did not specifically identify the potential harm(s) that might result from this incident, but its notification to affected individuals asked them to "monitor your … online account for suspicious activity. Promptly change the username and password for all other online accounts for which you use the same or similar username and password." In my view, a reasonable person would consider that the contact information and email address, particularly in conjunction with the fact that individuals are customers of the Organization, could be used to send unsolicited emails and for phishing purposes, leading to an increased risk of 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 did not provide its assessment of the likelihood of harm resulting from this incident. In my view, a reasonable person would consider the risk of harm resulting from this incident is increased as it resulted from a deliberate action (credential stuffing attack). The Organization reported that the credentials were used to access user accounts illegally and without authorization. The attacks appear to have been ongoing for approximately four hours before the Organization discovered the threat.

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 information and email address, particularly in conjunction with the fact that individuals are customers of the Organization, could be used to send unsolicited emails and for phishing purposes, leading to an increased risk of identity theft and fraud. These are significant harms.

The risk of harm resulting from this incident is increased as it resulted from a deliberate action (credential stuffing attack). The Organization reported that the credentials were used to access user accounts illegally and without authorization. The attacks appear to have been ongoing for approximately four hours before the Organization discovered the threat.

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 affected individuals were notified by letter on December 4, 2020 in accordance with the Regulation. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner