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 (Organization)
Decision number (file number)	P2022-ND-052 (File #022138)
Date notice received by OIPC	July 6, 2021
Date Organization last provided information	July 6, 2021
Date of decision	August 29, 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 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, • email address, • postal address (if entered), • birth day and month, • telephone number, and • last four digits of the payment card used (If the customer elected to save payment card information through the account, it would have been visible on the checkout/payment page.) This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported, "Purchases made in VS stores are not impacted by this issue. Additionally, to the extent the customer had a VS Credit Card account, the incident did not involve access to that account."

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• Between June 5, 2021 and June 6, 2021, the Organization learned that an unauthorized party gained access to personal information in certain online accounts. • The Organization determined that the unauthorized access to the online accounts was caused by a credential stuffing bot attack. • The Organization reported that the incident did not arise based on a breach of its security safeguards. It reported that the incident involved the apparent reuse of credentials (usernames and passwords) that may have been obtained in third-party hacking incidents in an attempt to access the online accounts of its users who use the same username and password on multiple websites.
Affected individuals	The incident affected 17 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Maintains, and is continuing to enhance, a documented information security program with numerous controls to detect and mitigate cyber attacks. • Promptly took steps to secure the accounts and determine the nature of the issue. • Asked affected individuals to create a new password. • Further refining its bot mitigation tool. • Completed the design work for self-service online account verifications that will notify customers of changes made to their online accounts, as well as email validation when new online accounts are created.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on July 6, 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.	In its report of the incident, the Organization did not specifically identify harms that might result from this incident. However, in the letter and notification to affected individuals, the Organization said: *Please monitor your… online account and, if applicable, any linked payment card 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. Call us if you have questions or concerns, or need assistance. In my view, a reasonable person would consider that contact information, and particularly email addresses, in association with the individual's relationship to the Organization, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Confirmed credentials could be used to compromise other 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.	In its report of the incident, the Organization did not specifically provide an assessment of the likelihood of significant harm resulting. In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the incident was the result of a deliberate, credential stuffing attack. The Organization reported that credentials were confirmed and could be used to access user accounts without authorization. The attacks appear to have been ongoing for approximately two (2) days 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.

The contact information, and particularly email addresses, in association with the individual's relationship to the Organization, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Confirmed credentials could be used to compromise other online accounts. These are significant harms.

The likelihood of harm resulting from this incident is increased as the incident was the result of a deliberate, credential stuffing attack. The Organization reported that credentials were confirmed and could be used to access user accounts without authorization. The attacks appear to have been ongoing for approximately two (2) days before the Organization discovered the threat.

I require the Organization to notify the affected individuals whose 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 letter on July 6, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Information and Privacy Commissioner