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	LUS Brands Inc. (Organization)
Decision number (file number)	P2020-ND-161 (File #015783)
Date notice received by OIPC	May 8, 2020
Date Organization last provided information	May 8, 2020
Date of decision	November 24, 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 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 a Canadian corporation selling hair products throughout North America and internationally, and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved email addresses. 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 uses a service provider, Klaviyo Inc., to help deploy email to the Organization's clients. • On March 5, 2020, the Organization was made aware that Klaviyo suffered a security breach incident, which occurred between November 13-29, 2019. • An unauthorized third party was able to manipulate parameters associated with URLs for Klaviyo's "unsubscribe" and "update subscription" functions. This resulted in a successful auto-population of fields within these forms with personal information the unauthorized third party was not authorized to receive.

	• The Organization reported it has not received any indication that any third party is using the email addresses.
Affected individuals	The incident affected 401 email addresses, including those of two (2) individuals residing in Alberta
Steps taken to reduce risk of harm to individuals	The Organization: • Immediately investigated and followed-up with additional questions to its service provider about the scope of the incident. • Notified affected individuals of the incident and recommended vigilance against potential phishing emails. • Safeguarding personal information to help prevent similar incidents in the future. The service provider: • Secured its systems to prevent the vulnerability from being re-exploited. • Responded to Organization's questions.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on March 24, 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.	In its notification to affected individuals, the Organization stated: *Critically, no other information was available to the unauthorized third party (only email address), so we are simply asking you to be vigilant against spam and phishing emails, particularly the ones that ask you for personal information.* In my view, a reasonable person would consider that, particularly when combined with an individual's name, email addresses 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 did not provide its assessment of the likelihood that harm may result from this incident, but its notification to affected individuals stated: *We have no reason to believe this information is being used by any third party, but please remember that [the Organization] will not contact you by email with hyperlinks requesting payment card details or other sensitive personal information. If you would ever like to confirm the validity of any …emails, please contact us.*

	In my view, a reasonable person would consider the likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to a deliberate unauthorized intrusion by an unauthorized third party. Further, the Organization can only assume that the unauthorized third party did not or will not misuse, disseminate or otherwise make the personal information at issue publicly available.

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, particularly when combined with an individual's name, email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to a deliberate unauthorized intrusion by an unauthorized third party. Further, the Organization can only assume that the unauthorized third party did not or will not misuse, disseminate or otherwise make the personal information at issue publicly available.

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 notified the affected individuals by email on March 24, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner