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	Namaste Technologies, Inc. (Organization)
Decision number (file number)	P2020-ND-104 (File #015209)
Date notice received by OIPC	June 24, 2019
Date Organization last provided information	June 24, 2019
Date of decision	September 23, 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 company that facilitates medical cannabis prescriptions by connecting eligible individuals in Canada to independent healthcare providers". 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 a list of names and email addresses for individuals who have expressed an interest in receiving information from the Organization. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On May 9, 2019, an employee of the Organization noticed unsolicited emails had been received at internal email addresses. • The Organization investigated and found that between May 4-8, 2019, a series of emails were sent to approximately 10,000 subscribers by a third party email services provider used by the Organization.

	• The emails did not originate from the Organization's account with the email services provider but instead came from the account of an employee of the Organization. • The employee claimed that the information was uploaded by accident. However, the Organization notes that the employee had separate business interests from those of the Organization and believes the incident may have been a deliberate attempt to solicit business using the Organization's information. • The employee confirmed the information was not used for any purpose other than to send the emails.
Affected individuals	The incident affected 10,000 individuals, including 264 in Alberta.
Steps taken to reduce risk of harm to individuals	• Contacted the email services provider and locked access to the account used to send the emails, prevented the sending of further emails from the account, and deleted the email addresses associated with the account. • Suspended the employee who uploaded the information (the employee has since resigned). • Reviewed systems to ensure there have been no further breaches of security, or other unauthorized exports of data. • Retaining a security firm to review and revise internal data control and security policies. • Implementing a technological security program that would include the ability to detect and block exports of information. • Undertaking a new round of employee training to ensure employees are informed of their obligation to protect personal information.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on June 21, 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 "The unauthorized disclosure of names and email addresses has the potential to expose the individuals to an increase in unsolicited/spam email, and can also potentially lead to phishing." I agree with the Organization's assessment. A reasonable person would consider that the information at issue could be used for phishing purposes, 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	The Organization reported the information… *…has been used to send the individuals on the list advertising for an unlicensed cannabis dispensary.*

or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	*However, the email services provider used to send the unsolicited Emails has confirmed that they have deleted the [information] from the account used to send such Emails. Further, the employee involved in the incident has stated the matter was accidental, and that they did not disclose the [information] other than to the Account, and did not use [it]… for purposes other than sending the Emails.* *[The Organization] has not received further unauthorized email to the Test Addresses …[and] it would be difficult for a third party to identify which addresses where [sic] Test Addresses, and which are not. As a result, [the Organization] believes the incident to be contained.* In my view, a reasonable person would consider that the likelihood of harm is increased because the Organization cannot be sure the incident was not deliberate, and the information was in fact used to send advertising for an unlicensed cannabis dispensary. The Organization confirmed the information was not used for purposes other than to send the emails; however, it is not clear from the Organization's report that it confirmed the information was not copied and cannot be used in future.

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 information at issue could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm is increased because the Organization cannot be sure the incident was not deliberate, and the information was in fact used to send advertising for an unlicensed cannabis dispensary. The Organization confirmed the information was not used for purposes other than to send the emails; however, it is not clear from the Organization's report that it confirmed the information was not copied and cannot be used in future.

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 the affected individuals by email on June 21, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner