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	NeuroTrition Inc. (Organization)
Decision number (file number)	P2021-ND-159 (File #018138)
Date notice received by OIPC	November 18, 2020
Date Organization last provided information	November 18, 2020
Date of decision	August 25, 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 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 operates in Alberta and 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: • first name, • email address, and • health care practitioner status. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On or about October 3, 2020, the Organization was informed that an account held with "Mail Chimp" had been closed. • The Organization learned that a former contractor had accessed the account without authorization, closed it without the Organization's knowledge, and retained account information from Mail Chimp without the Organization's knowledge or consent, on or about September 29 - October 3, 2020.

	• The Organization reported that there is no evidence that the Organization's membership information was exported externally; however, it is possible that lists were viewed by the former contractor. • The Organization reported that it is not aware of any use of these lists by the former contractor and not aware of any other activities (malicious or otherwise) undertaken by the former contractor.
Affected individuals	The incident affected 1,937 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Set up two-factor authentication. • Set up further verification measures via additional questions. • Reset all passwords. • Sending a Cease and Desist letter to the former contractor. • Notifying police if anything malicious upon receipt of the Cease and Desist letter. • Will routinely reset business passwords and will reset passwords immediately upon notifying any future contractor or employee of termination from the Organization.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on November 17, 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.	The Organization reported: *It is possible that these lists were viewed by the Former Contractor when they accessed our account without authorization. We are not aware of any use of these lists by the Former Contractor, other than what has been reported above. We are also not aware of any other activities (malicious or otherwise) undertaken by this Former Contractor.* *We report this potential breach out of an abundance of caution.* In my view, a reasonable person would consider that names and email addresses, along with status as a health care practitioner, could be used for the purposes of phishing, increasing the affected individuals' 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 reported that "The likelihood that harm will result is low, but we want to report this out of an abundance of caution." In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the information was accessed without the Organization's knowledge or authorization. It is not clear whether the Organization requested and/or confirmed that the unauthorized third party delete the personal information and not use, make copies, further disclose, or otherwise distribute the personal information. The Organization reported that it has no evidence that the Organization's membership information was exported externally; however, it is possible that these lists were viewed by the former contractor. I do not find this reassuring, however, as an unauthorized third party accessed the personal information at issue and the Organization felt it necessary to send a Cease and Desist letter to the unauthorized third party.

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 names and email addresses, along with status as a health care practitioner, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident is increased because the information was accessed without the Organization's knowledge or authorization. It is not clear whether the Organization requested and/or confirmed that the unauthorized third party delete the personal information and not use, make copies, further disclose, or otherwise distribute the personal information. The Organization reported that it has no evidence that the Organization's membership information was exported externally; however, it is possible that these lists were viewed by the former contractor. I do not find this reassuring, however, as an unauthorized third party accessed the personal information at issue and the Organization felt it necessary to send a Cease and Desist letter to the unauthorized third party.

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 November 17, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner