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	Neptune Wellness Solutions Inc. (Organization)
Decision number (file number)	P2020-ND-092 (File #016528)
Date notice received by OIPC	July 27, 2020
Date Organization last provided information	July 27, 2020
Date of decision	September 1, 2020
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual 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 all or some of the following information: • name, • email address, • home address, • date of birth, • benefits information, • social insurance number, • driver's license number, and • passport number. 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 July 15, 2020, the Organization received a message claiming that its networks were hacked and all of the Organization's files, documents, photos, databases and other important data had been encrypted, making them inaccessible. The message also claimed that certain private data from the Organization's network had been downloaded. • The unknown actor threatened to post information and publicize if the Organization failed to respond and purchase the encryption key. • The Organization believes that it is possible that information contained in certain employee files were downloaded.
Affected individuals	The incident affected 345 individuals in Canada, of which 1 is an Alberta resident.
Steps taken to reduce risk of harm to individuals	• Hired a third party cyber security firm to assist with the investigation, resolve the issue, recover information and identify the information that was compromised. • Offered current and former employees and board members free credit monitoring and identity theft prevention.
Steps taken to notify individuals of the incident	Affected individuals were notified on July 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.	The Organization reported that it "identified a potential risk of harm of phishing, identity theft and fraud in relation to the incident." I agree with the Organization's assessment. A reasonable person would consider the contact and identity information at issue could be used to cause the significant harms of identity theft, and fraud. Email address could be used for phishing, increasing vulnerability to identity theft and fraud.
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 specifically assess the likelihood of harm resulting from this incident, but said it "… believes that it is possible that information contained in certain… employment files have been downloaded by the actor." In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion, ransom demand). In addition, personal information may have been downloaded and stolen.

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 individual. A reasonable person would consider the contact and identity information at issue could be used to cause the significant harms of identity theft, and fraud. Email address could be used for phishing, increasing vulnerability to identity theft and fraud. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion, ransom demand). In addition, personal information may have been downloaded and stolen. I require the Organization to notify the affected individual 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 individual on July 24, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner