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	Novo Nordisk Canada Inc. (Organization)
Decision number (file number)	P2022-ND-016 (File #022281)
Date notice received by OIPC	April 12, 2021
Date Organization last provided information	April 12, 2021
Date of decision	April 7, 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 those 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. The Organization's head office is in Mississauga, Ontario.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • email address, • username, and • password. 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	• The Organization contracts with Limeade, a third party service provider, to offer the NovoHealth platform to employees. • The platform allows employees to track activities to earn rewards in the form of gift cards. • In late September 2020, Limeade discovered a third party used automated means to guess usernames and passwords to gain

	unauthorized access to end users' accounts. Limeade made product changes and the suspicious activity subsided. • In November 2020, Limeade became aware of some atypical email resets, user accounts unexpectedly "leveling up," and anomalies in gift card redemptions. • Gift card rewards were sent to fraudulently created email accounts and cashed in by the unknown third party. In some cases, gift card codes were fraudulently obtained from the user account directly upon a "level up." • Limeade's ongoing monitoring detected continued attempts to access accounts by validating usernames and passwords in January and February 2021. Some accounts were re-compromised. Limeade reset the passwords again.
Affected individuals	The Organization reported the incident affected five (5) Canadians, including two (2) whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	<u>Limeade:</u> • Partnered with a third party forensics firm to conduct a security incident investigation, including analysis of affected user account activity. • Increased monitoring and logging to flag any non-standard user behaviour or suspect domains. • Blocked duplicate email addresses from use. • Removed the ability for an end user to change the email address without its customer support staff. • Implemented a 15-minute account lockout after three failed password attempts and additional logging when this occurs. • Required CAPTCHA after an account lock-out and anytime it sees a username used from a new device. • Tuned the rules in its application firewall. • Forced a password reset on affected user accounts. • Notified customers. <u>Organization:</u> • Notified affected users and included best practices around passwords and the need to monitor/report any suspicious activity on accounts. • Confirmed that it expects Limeade to immediately notify the Organization's Privacy Officer of any suspected or confirmed privacy breaches in the future. • Continuing to work with Limeade to assess its privacy and security protocols.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on April 9, 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, *Email addresses could be used for the purposes of phishing. Usernames and passwords could be used to compromise an individual's other on-line accounts (credential stuffing) or for phishing/social engineering attacks.* In my view, a reasonable person would consider that contact and credential information could be used to cause the significant harms of identity theft, and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all 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: *There is a low risk of harm to individuals. Based on the forensics investigation conducted, it is clear that the bad actor's motivation for the attacks was to engage in gift card fraud rather than to misuse the personal information compromised.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). The information was exposed from the time the incident occurred to when it was discovered.

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 contact and credential information could be used to cause the significant harms of identity theft, and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of harm resulting from this incident is increased because personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). The information was exposed from the time the incident occurred to when it was discovered.

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 April 9, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance