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	Standard Nutrition Canada Co., owned by Sollio Agriculture, a division of La Coop federee (Organization)
Decision number (file number)	P2019-ND-194 (File #013296)
Date notice received by OIPC	May 16, 2019
Date Organization last provided information	May 16, 2019
Date of decision	December 13, 2019
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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The information at issue includes: • name, • address, • telephone number, • social insurance number, • bank account number, • date of birth, • gender, and • marital status. 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 April 6, 2019, an employee's email account was accessed by an unauthorized individual through a phishing scam asking for login credentials. The email account was then used to send similar phishing messages to other employee accounts on April 9, 2019. • As a result, two other employee email accounts were accessed by an unauthorized individual. These accounts were blocked quickly enough they were not used to send phishing messages. • Only one of the email accounts that was accessed included personal information.
Affected individuals	The incident affected 2 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Secured the affected accounts, and investigated. • Required the affected employee to permanently delete the two e-mails containing personal information. • Changed the three employees' compromised email account passwords. • Activated a multi-factor authentication for all mail account users. • Activated a malware filter on email accounts. • Setting up application impersonation for internal mailing server. • Extensively monitoring for any further intrusions. • Providing awareness-raising campaign and mandatory training about cybersecurity for all employees. • Offered the affected individuals a one-year credit bureau subscription at no cost.
Steps taken to notify individuals of the incident	Affected individuals were notified by email April 23, 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 that "…the nature of the personal information concerning the employee that may have been accessed makes possible that the harm could include identity theft or fraud". In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses 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 or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported that "…there is a low risk of harm to the two Alberta residents resulting from this incident. There is no evidence that personal information has been accessed, used or communicated". In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing email) and the Organization reported "that only one of the email accounts that were accessed by the unauthorized individual included personal information". The Organization did not provide any information to suggest that, once accessed, the information was not exfiltrated or otherwise copied or distributed. The accessed account was in fact used to send subsequent phishing emails.

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 contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing email) and the Organization reported "that only one of the email accounts that were accessed by the unauthorized individual included personal information". The Organization did not provide any information to suggest that, once accessed, the information was not exfiltrated or otherwise copied or distributed. The accessed account was in fact used to send subsequent phishing emails.

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 individuals were notified by email April 23, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner